AVAYA

INTELLIGENT COMMUNICATIONS

ASM & SMGR 6.2

Avaya Aura® System Manager and Session Manager Administration

Please note that this course does not have audio. Click the forward/backward arrows to navigate this course.

Course Duration: 4 Days

AVAYA | LEARNING

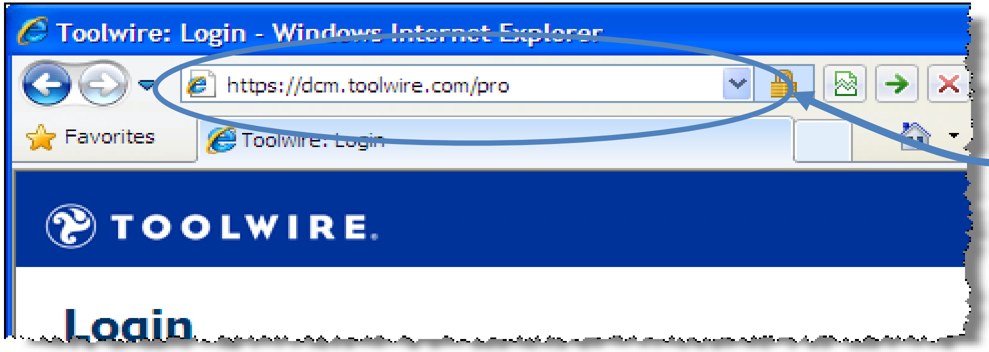
Module 01: Connecting Student Computer to Toolwire Network

Three step process:

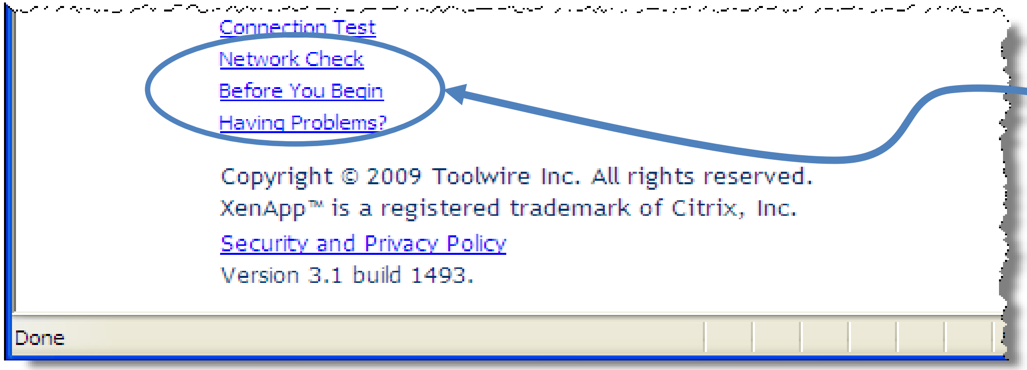
- Use browser to log in to Toolwire
- Follow the steps to install the Citrix ICA Web Client
- Enter your Toolwire Login and Password

Module Duration: 45 minutes

Classroom Setup


Toolwire: Login - Windows Internet Explorer
https://dcm.toolwire.com/pro
Favorites
Toolwire: Login
TOOLWIRE.
Login

Navigate to the Toolwire portal

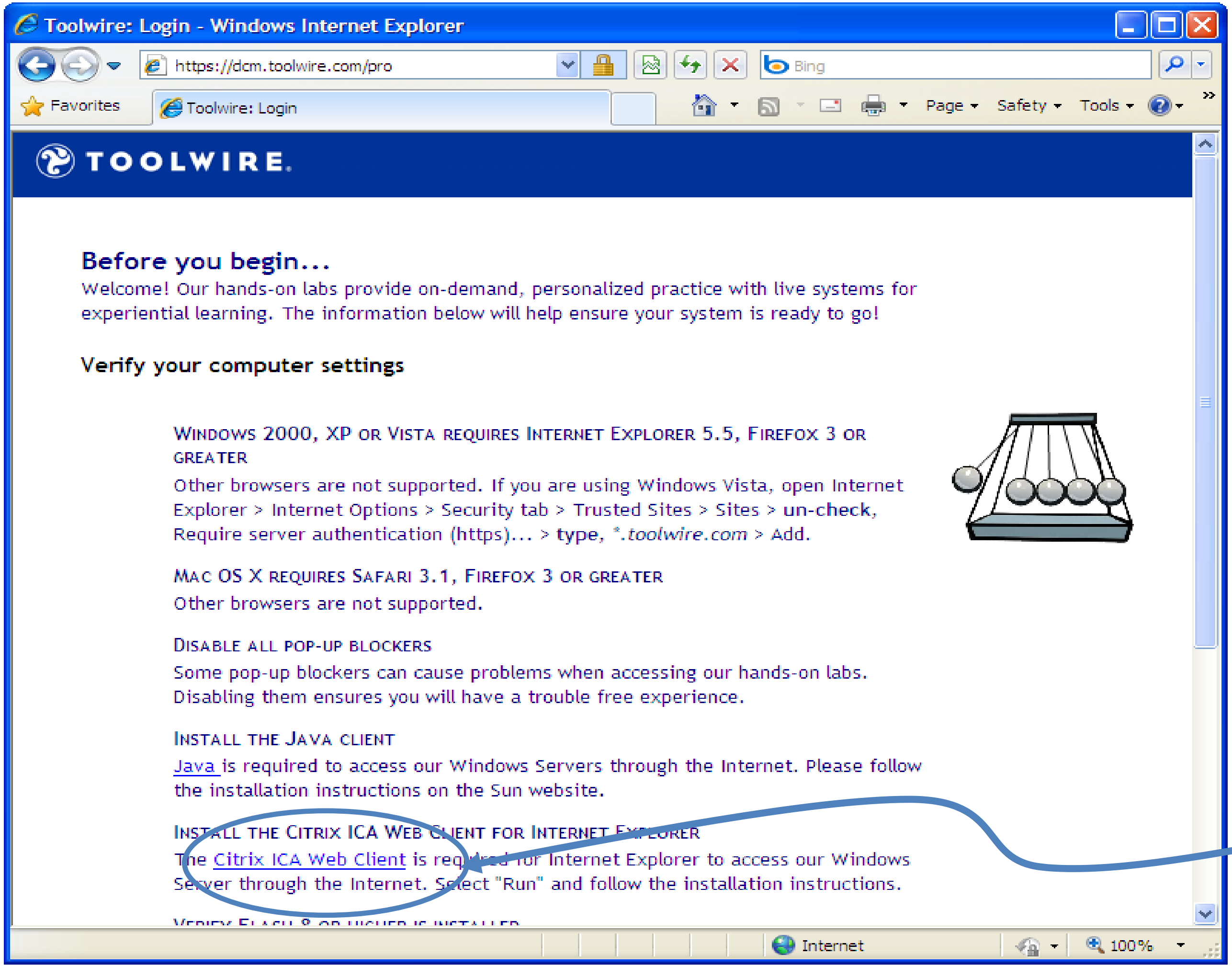


Copyright © 2009 Toolwire Inc. All rights reserved.
XenApp™ is a registered trademark of Citrix, Inc.

Version 3.1 build 1493.

You should have already downloaded the Citrix client – if not, click 'Before You Begin'

Classroom Setup


Toolwire: Login - Windows Internet Explorer
https://dcm.toolwire.com/pro
Bing
Favorites
Toolwire: Login
Page
Safety
Tools
TOOLWIRE.
Internet
100%

Before you begin...

Welcome! Our hands-on labs provide on-demand, personalized practice with live systems for experiential learning. The information below will help ensure your system is ready to go!

Verify your computer settings

WINDOWS 2000, XP OR VISTA REQUIRES INTERNET EXPLORER 5.5, FIREFOX 3 OR GREATER

Other browsers are not supported. If you are using Windows Vista, open Internet Explorer > Internet Options > Security tab > Trusted Sites > Sites > un-check, Require server authentication (https)... > type, *.*toolwire.com* > Add.

MAC OS X REQUIRES SAFARI 3.1, FIREFOX 3 OR GREATER

Other browsers are not supported.

DISABLE ALL POP-UP BLOCKERS

Some pop-up blockers can cause problems when accessing our hands-on labs. Disabling them ensures you will have a trouble free experience.

INSTALL THE JAVA CLIENT

Java is required to access our Windows Servers through the Internet. Please follow the installation instructions on the Sun website.

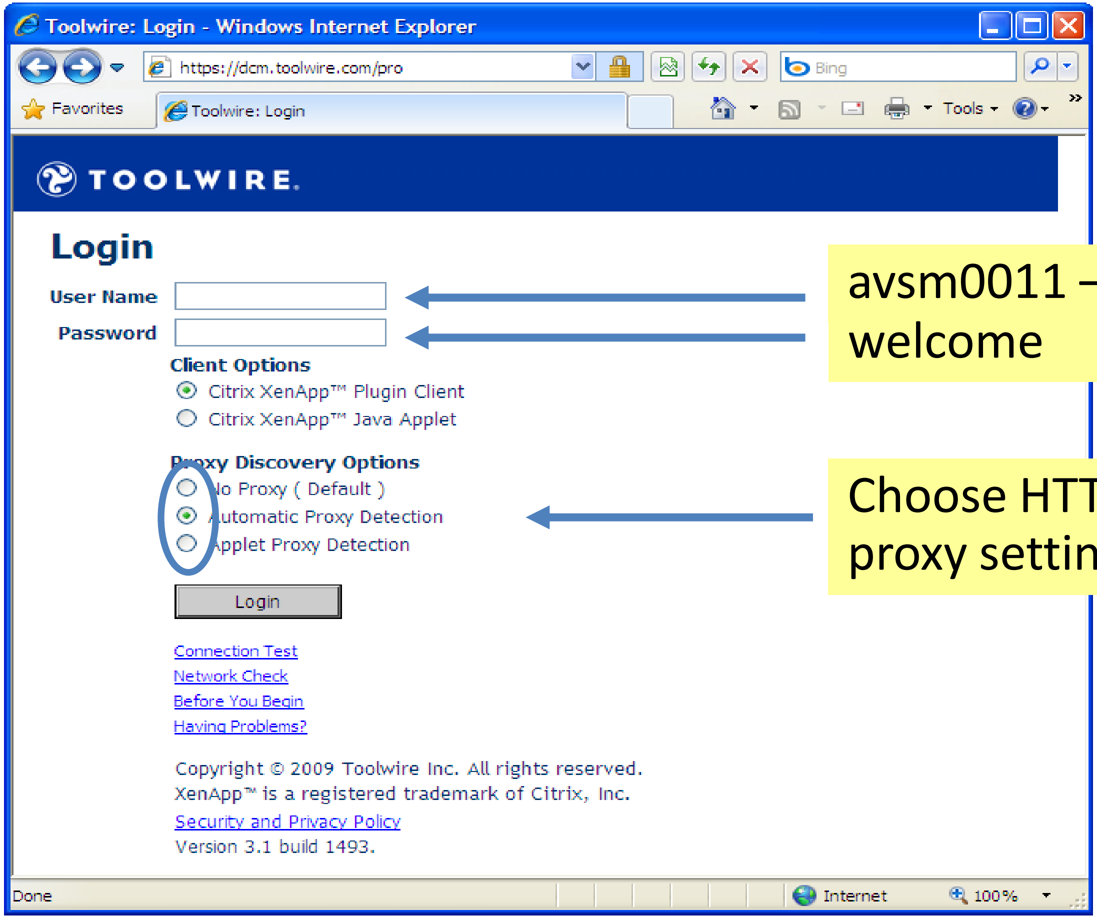
INSTALL THE CITRIX ICA WEB CLIENT FOR INTERNET EXPLORER

The Citrix ICA Web Client is required for Internet Explorer to access our Windows Server through the Internet. Select "Run" and follow the installation instructions.

VERIFY FLASH 8 OR HIGHER IS INSTALLED

Follow the steps, including installing the Citrix ICA Web Client

Classroom Setup


Toolwire: Login - Windows Internet Explorer
https://dcm.toolwire.com/pro
Bing
Favorites
Toolwire: Login
Tools
TOOLWIRE.
Done
Internet
100%

Login

User Name

Password

Client Options

● Citrix XenApp™ Plugin Client

○ Citrix XenApp™ Java Applet

Proxy Discovery Options

○ No Proxy (Default)

● Automatic Proxy Detection

○ Applet Proxy Detection

Login

Connection Test

Network Check

Before You Begin

Having Problems?

Copyright © 2009 Toolwire Inc. All rights reserved.
XenApp™ is a registered trademark of Citrix, Inc.

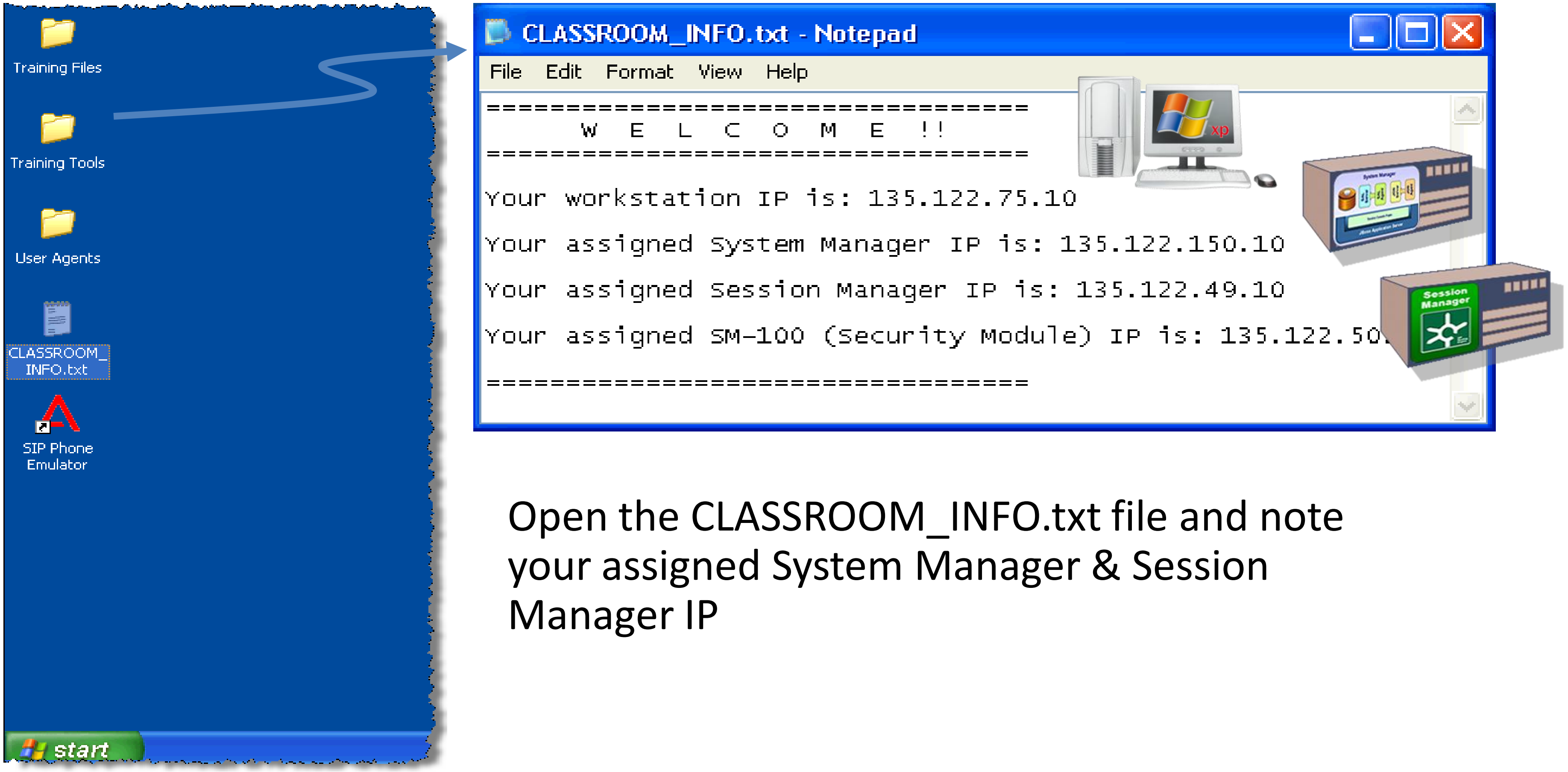
Security and Privacy Policy

Version 3.1 build 1493.

avsm0011 – 17 (provided by Instructor)
welcome

Choose HTTP proxy settings

Toolwire Lab

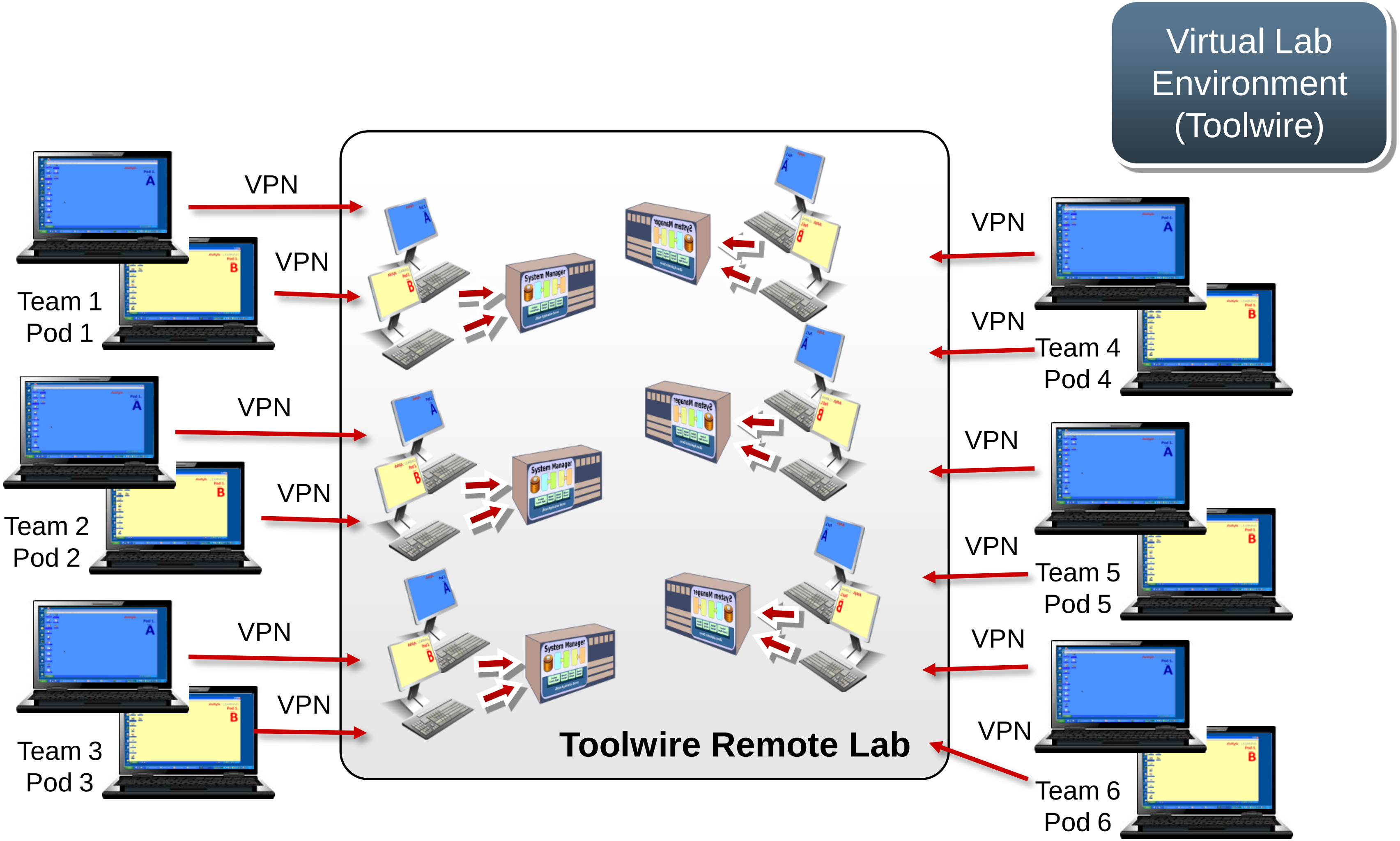


```
==================================
      W  E  L  C  O  M  E  !!
==================================

Your workstation IP is: 135.122.75.10

Your assigned System Manager IP is: 135.122.150.10

Your assigned Session Manager IP is: 135.122.49.10

Your assigned SM-100 (Security Module) IP is: 135.122.50.

==================================
```

Open the CLASSROOM_INFO.txt file and note your assigned System Manager & Session Manager IP

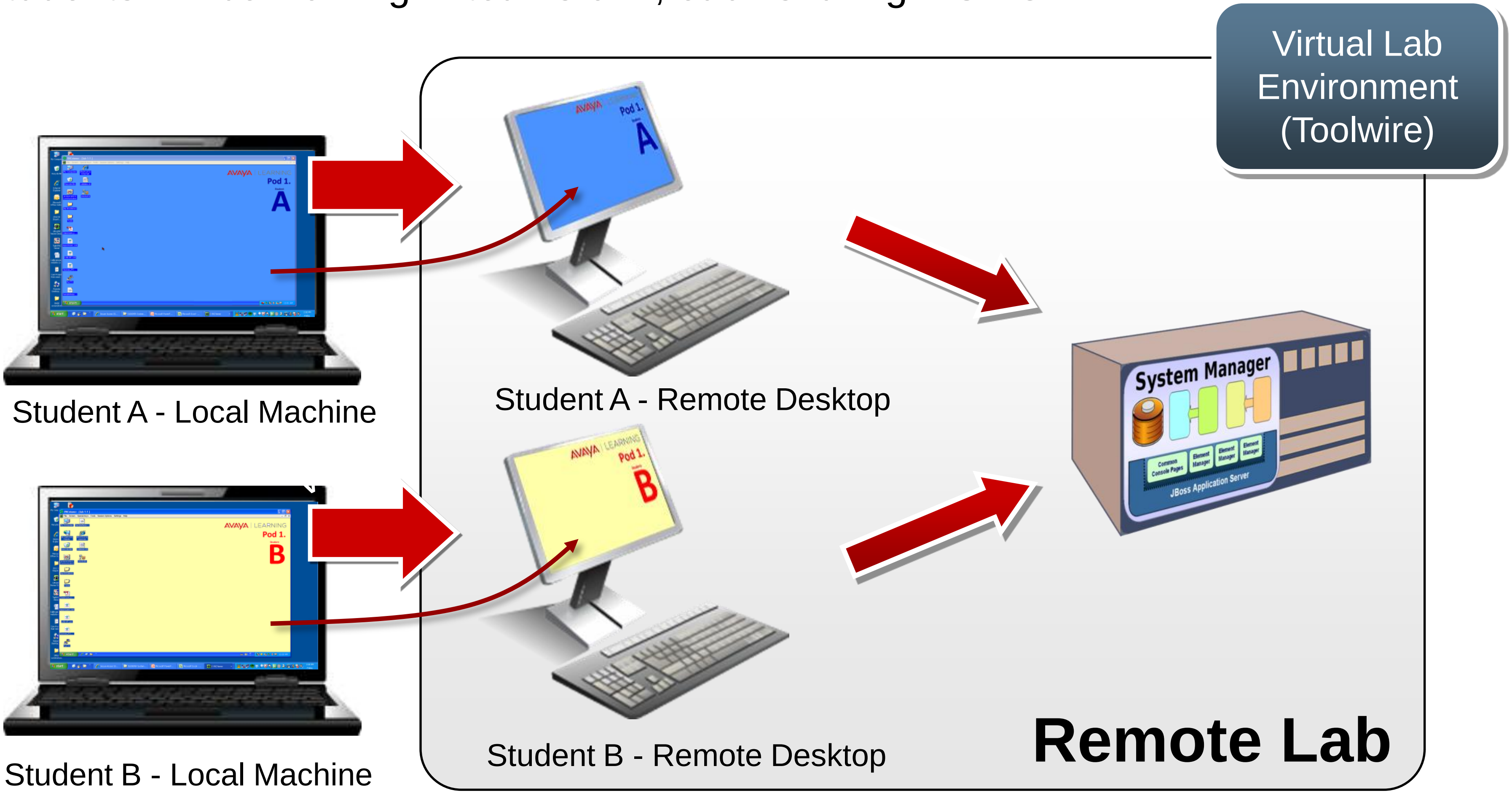
SMGR Virtual Lab

The lab caters for 6 teams of 2 students. Each team has their own SMGR.



SMGR Virtual Lab

Students will be working in teams of 2, each sharing 1 SMGR.



Virtual Lab Environment (Toolwire)

Student A - Local Machine

Student A - Remote Desktop

Student B - Local Machine

Student B - Remote Desktop

Remote Lab

VPN = Virtual Private Network

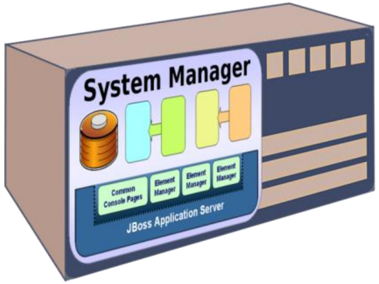
VNC = Virtual Network Computing

SMGR Equipment Setup

Physical Environment (Travel Kit)

Classroom Desktop

Classroom Desktop



We'll be sharing access to the available servers

- We'll need to partner up

AVAYA | LEARNING

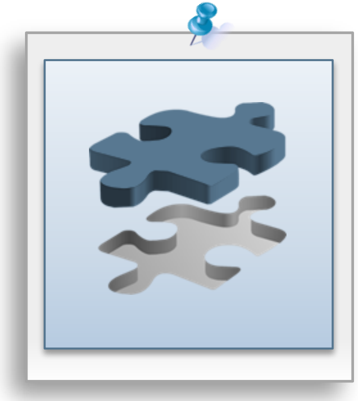
Module 02: System Manager Features & Benefits

Lesson Duration: 15 minutes

Lesson Objectives

After completing this lesson, you will:

- Recall SMGR's place in the Aura network.



Lesson Duration: 15 Minutes

What part does SMGR play in

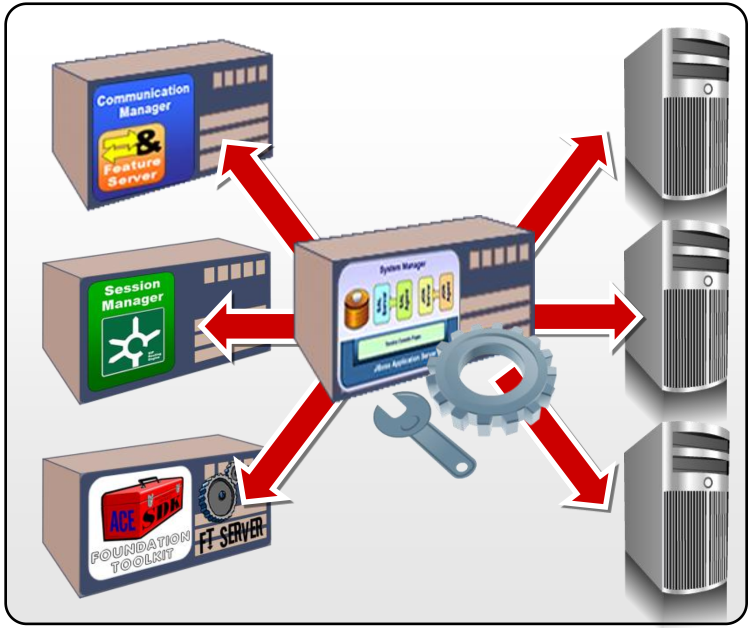
AVAYA

aura™

???

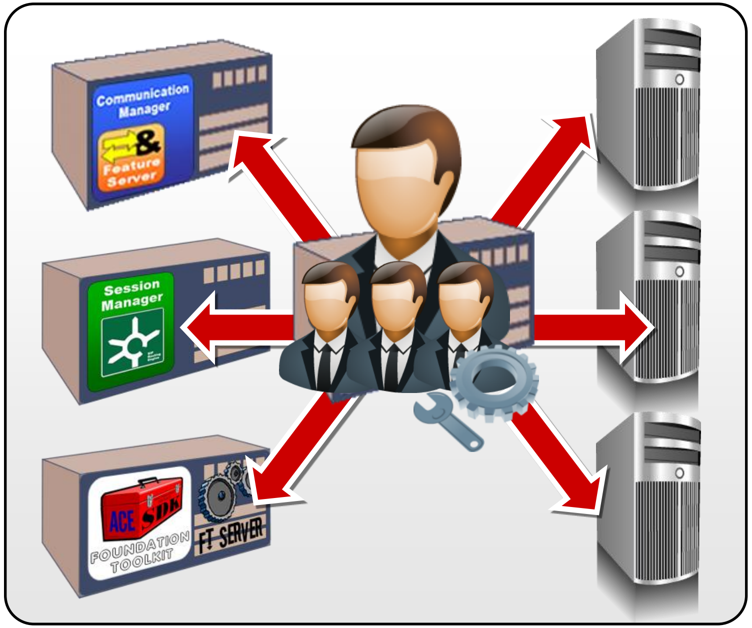
SMGR in Avaya Aura®

- Centralized Product Management



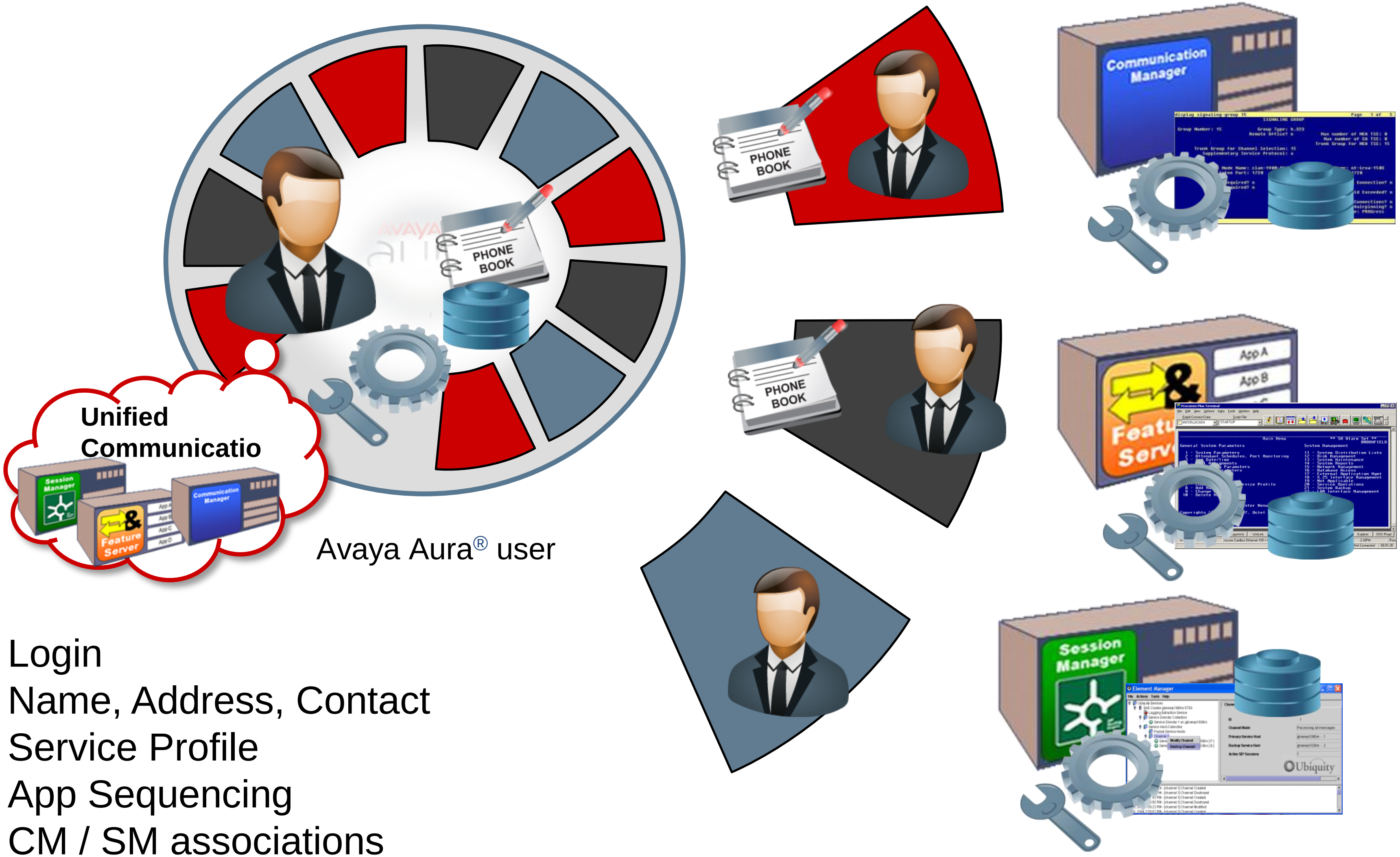
- Administration
- Configuration
- Licensing

- User Profile Management
  - Administrators / communication users



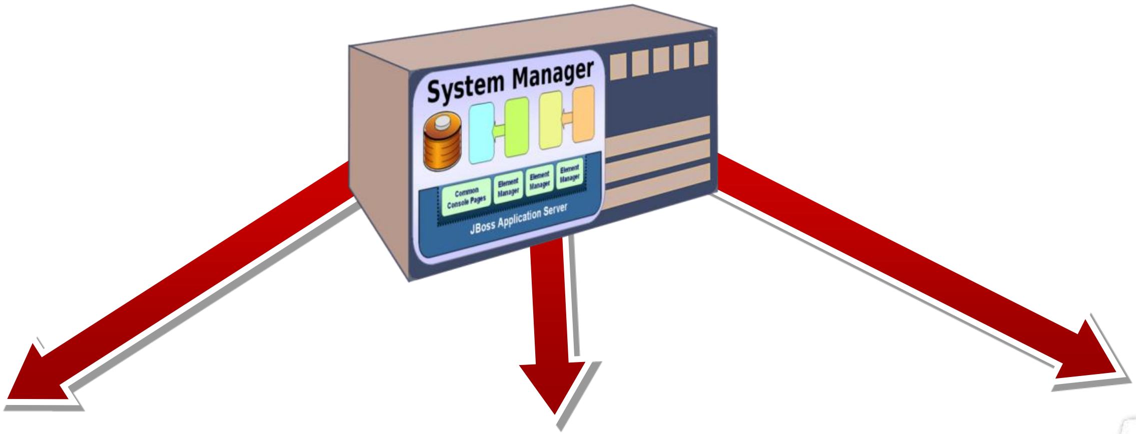
- Central User Profile
- User info shared
- RBAC – Role Based Access Control

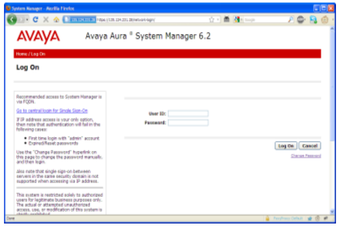
Avaya Aura® User Profiles



- Login
- Name, Address, Contact
- Service Profile
- App Sequencing
- CM / SM associations

SMGR – Additional Roles & Key Functions




System Manager - Mozilla Firefox
https://135.124.231.28/network-login/
AVAYA

Avaya Aura ® System Manager 6.2

Home / Log On

Log On

Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is

User ID:
Password:

Single sign-on to central management interface

Event & alarm monitoring, SNMP (Simple Network Management Protocol).
Remote maintenance using Secure Access Link (SAL)

Certificate Authority (CA) enabling secured network communication.
Integrated WebLM for licensing.

SMGR Specification – Capacity

Capacities	SMGR 5.2	SMGR 6.0	SMGR 6.1	SMGR 6.2
Number of administrator logins	50	250	250	250
Number of simultaneous logins	10	50	50	50
Number of endpoints (total)	25,000	100,000	100,000	250,000
Number of SIP endpoints	25,000	100,000	100,000	100,000
Number of end users	25,000	100,000	100,000	250,000
Number of contacts per user	250*	250*	250*	250*
Number of public contacts	1,000	1,000	1,000	1,000
Number of personal contact lists, per user	1	1	1	1
Number of members in a personal contact list	250	250	250	250
Number of groups	50	300	300	300
Number of members in a group	300	400	400	400
Number of elements	10,000	25,000	25,000	25,000
Number of CMs (either as Feature Server or Evolution Server) (counts against the total number of elements)	100	500	500	500
Number of Branch Session Managers (counts against the total number of elements)	n/a	250	250	250
Number of B5800 Branch Gateways (counts against the total number of elements)	n/a	n/a	n/a	2,000

* There is a system limit of 2.5 million contact.

Note: 2000 requires several WebLM Servers

AVAYA | LEARNING

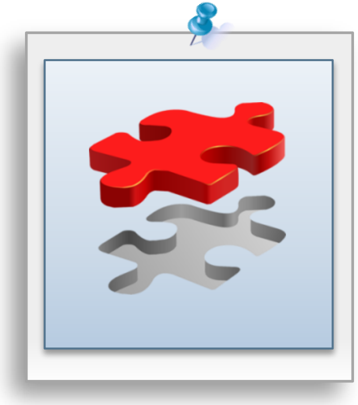
Module 03: System Manager User Administration

Module Duration: 3 hours

Module Objectives

After completing this module, you will be able to:

- Understand the relationship between SMGR users, roles & groups.
- Create groups of different types.
- Create & assign custom roles carrying specific resource permissions.



Module Duration: 3 Hours

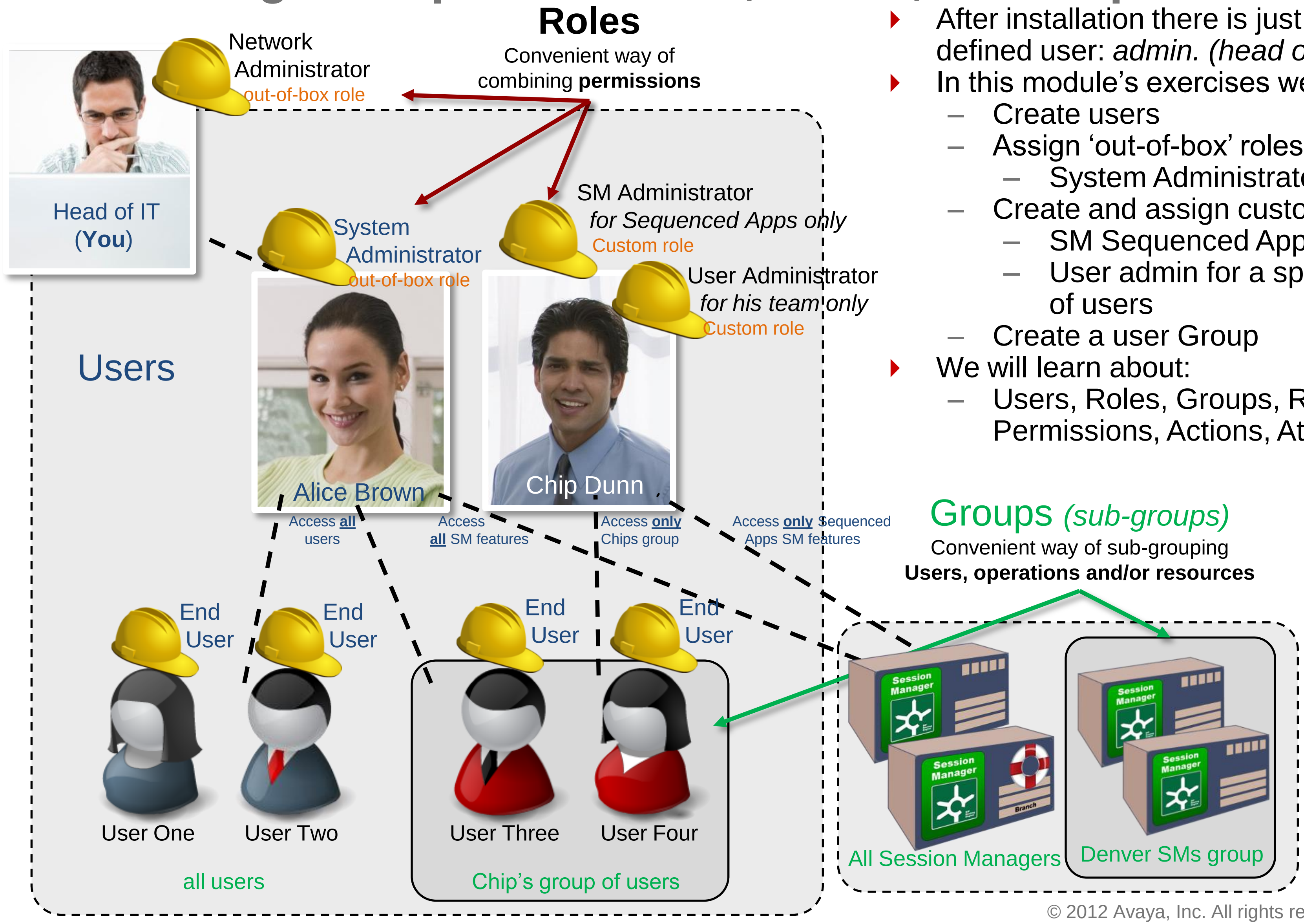
AVAYA | LEARNING

Module 3: System Manager User Administration

Lesson 01: Users, Roles, & Groups

Lesson Duration: 30 minutes

Our training Enterprise – Roles, Users, & Groups



Roles

Convenient way of combining **permissions**

Network Administrator
out-of-box role

Head of IT
(**You**)

Users

System Administrator
out-of-box role

SM Administrator
for Sequenced Apps only
Custom role

User Administrator
for his team only
Custom role

Alice Brown

Chip Dunn

Access **all** users

Access **all** SM features

Access **only** Chips group

Access **only** Sequenced Apps SM features

End User

End User

End User

End User

User One

User Two

User Three

User Four

all users

Chip's group of users

Groups *(sub-groups)*

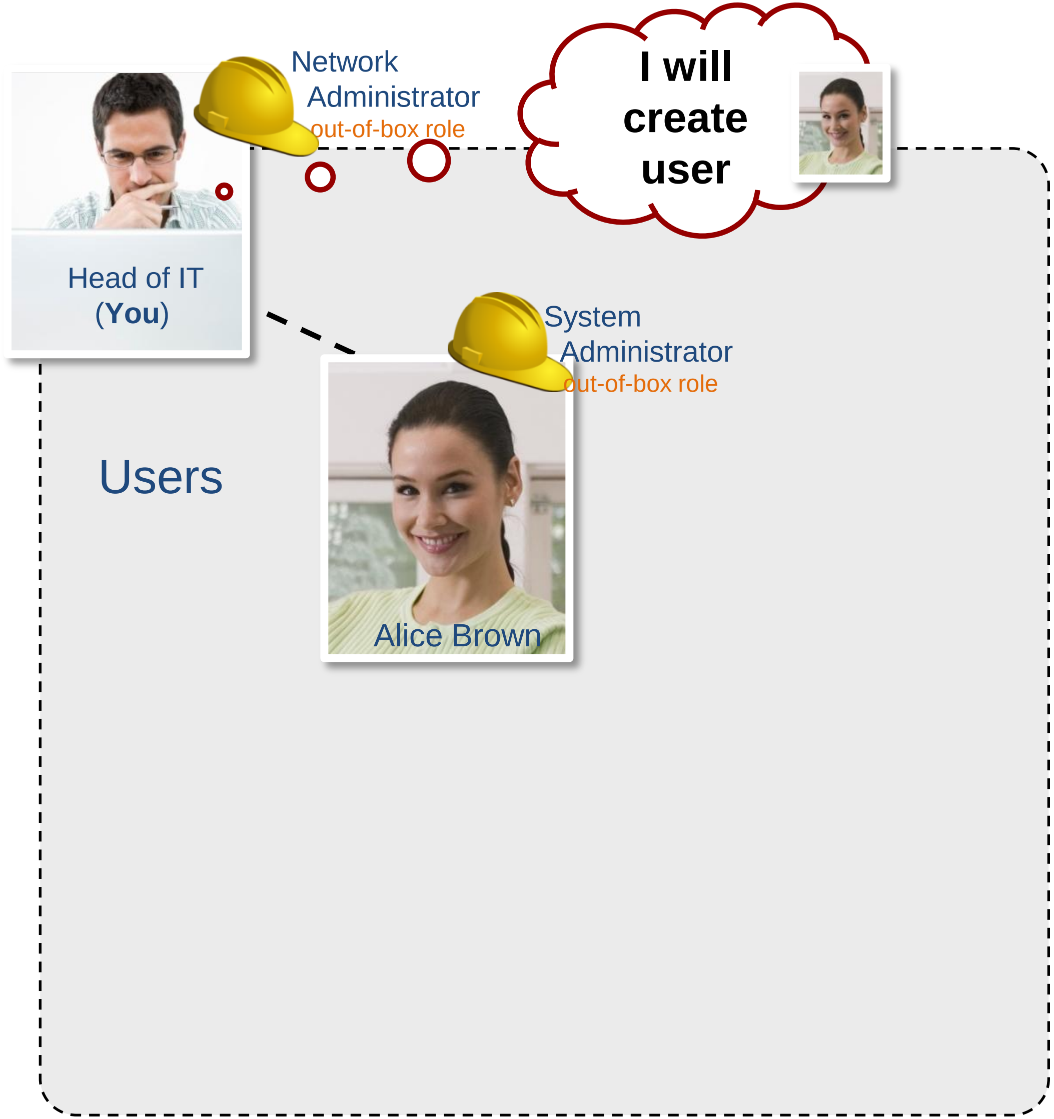
Convenient way of sub-grouping
Users, operations and/or resources

All Session Managers

Denver SMs group

- After installation there is just one defined user: *admin. (head of IT?)*
- In this module's exercises we will:
  - Create users
  - Assign 'out-of-box' roles
    - System Administrator
  - Create and assign custom roles
    - SM Sequenced Apps admin
    - User admin for a specific team of users
  - Create a user Group
- We will learn about:
  - Users, Roles, Groups, Resources, Permissions, Actions, Attributes

Topic 1: Create a User and Assign System Admin Role



Network Administrator
out-of-box role

Head of IT
(**You**)

I will create user

System Administrator
out-of-box role

Users

Alice Brown

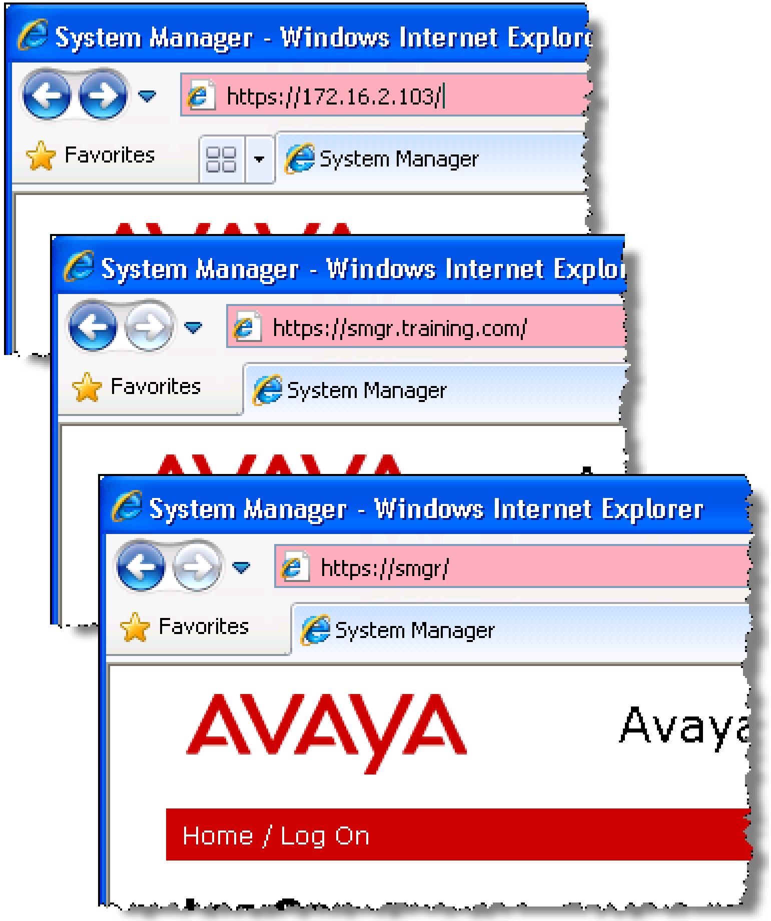
Whilst working on this topic we will learn…

- How to log in for the first time
  - including the mandatory change of password
- About navigating the System Manager interface
- About different types of user
- How to create a user
- About roles
  - What are they?
- How to assign an out-of-box role to a user

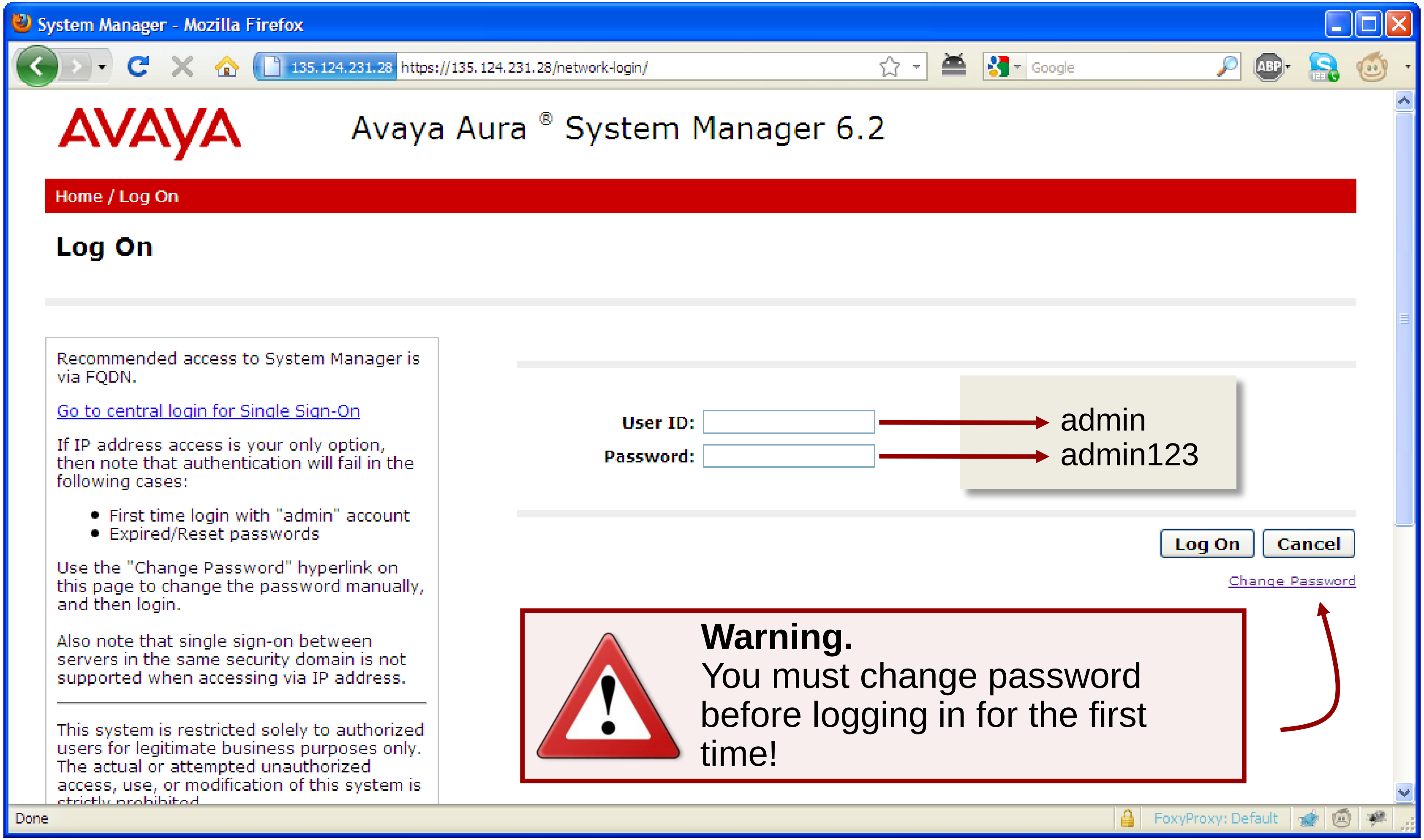
Logging in to SMGR – Login & URL

You may access the SMGR interface using…

- SMGR’s IP Address
- A fully qualified domain name (FQDN) that resolves to SMGR’s IP address
  - Assumes that SMGR has been registered with a domain name service (DNS)
- SMGR’s hostname


System Manager - Windows Internet Explore
https://172.16.2.103/
Favorites
System Manager
System Manager - Windows Internet Explo
https://smgr.training.com/
Favorites
System Manager
System Manager - Windows Internet Explorer
https://smgr/
Favorites
System Manager
AVAYA
Avaya
Home / Log On

Login – Change Password First


System Manager - Mozilla Firefox
135.124.231.28 https://135.124.231.28/network-login/
Google
AVAYA
Avaya Aura ® System Manager 6.2
Home / Log On

Log On

Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

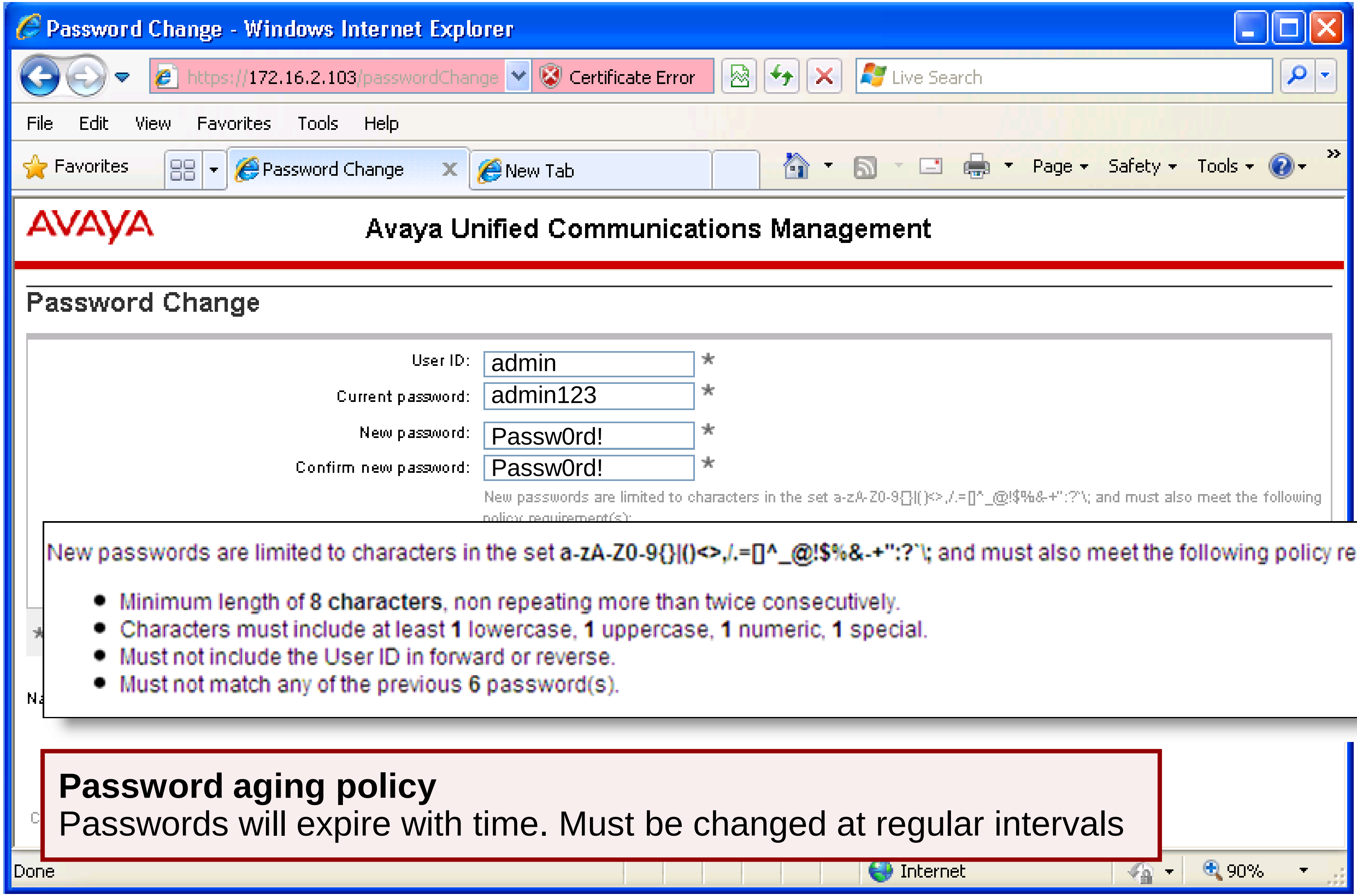
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited

User ID: → admin

Password: → admin123

Warning.
You must change password before logging in for the first time!

Changing Password



Password Change - Windows Internet Explorer
https://172.16.2.103/passwordChange
Certificate Error
Live Search
File Edit View Favorites Tools Help
Favorites
Password Change
New Tab
Page Safety Tools
Done
Internet
90%

AVAYA

Avaya Unified Communications Management

Password Change

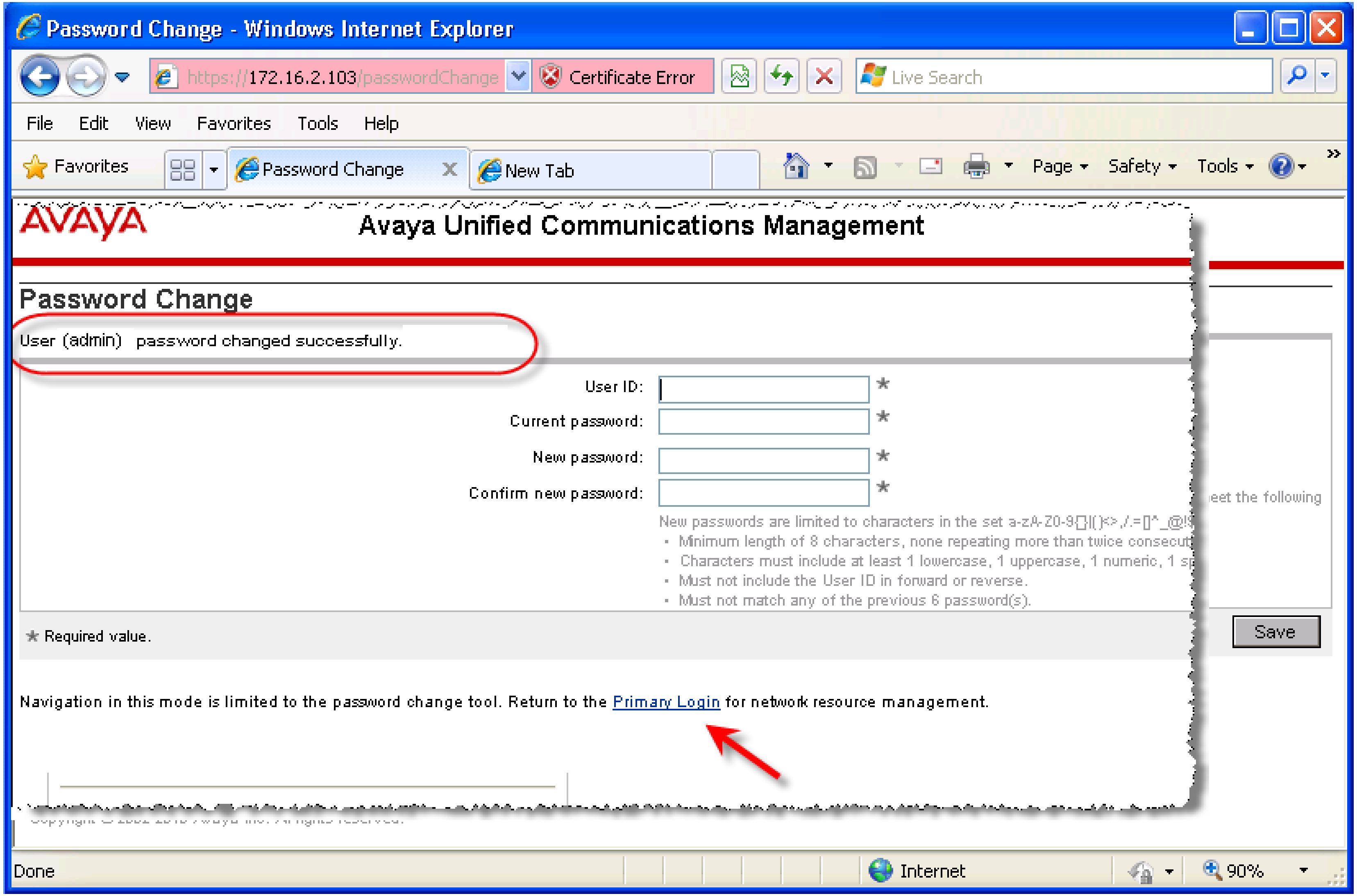
User ID:	admin	*
Current password:	admin123	*
New password:	Passw0rd!	*
Confirm new password:	Passw0rd!	*

New passwords are limited to characters in the set **a-zA-Z0-9{}|()<>,/.=[]^_@!$%&-+":?`\;** and must also meet the following policy requirement(s):

- Minimum length of **8 characters**, non repeating more than twice consecutively.
- Characters must include at least **1** lowercase, **1** uppercase, **1** numeric, **1** special.
- Must not include the User ID in forward or reverse.
- Must not match any of the previous 6 password(s).

Password aging policy
Passwords will expire with time. Must be changed at regular intervals

After Changing Password Go Back to Log In



Password Change - Windows Internet Explorer
https://172.16.2.103/passwordChange
Certificate Error
Live Search
File Edit View Favorites Tools Help
Favorites
Password Change
New Tab
Page Safety Tools
AVAYA
Avaya Unified Communications Management
Done
Internet
90%

Password Change

User (admin) password changed successfully.

User ID: *

Current password: *

New password: *

Confirm new password: *

...eet the following

New passwords are limited to characters in the set a-zA-Z0-9{}|()<>,/.=[]^_@!$

- Minimum length of 8 characters, none repeating more than twice consecut
- Characters must include at least 1 lowercase, 1 uppercase, 1 numeric, 1 sp
- Must not include the User ID in forward or reverse.
- Must not match any of the previous 6 password(s).

★ Required value.

Save

Navigation in this mode is limited to the password change tool. Return to the Primary Login for network resource management.

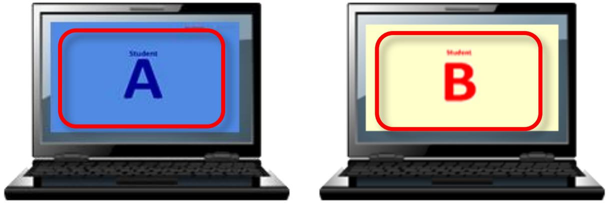
Exercise: Login to SMGR and Change Password

Objective & Outcome
The objective of this exercise is to learn how to log in to SMGR for the first time, and how to change the default password. By the time you are done, both students should be logged in to SMGR with the new password.

1. ONLY STUDENT A: Open a browser and enter the SMGR login URL for your assigned SMGR. Student B to shadow using second VNC session
   - **http://<SMGR hostname>.** Check the student lab guide for your SMGR hostname
   - E.g. **smgr-labx.training.com**
2. Click the ‘Change Password’ link (on the right) and change the admin password
   - Original password: **admin123**
   - Change to: **Passw0rd!**
3. BOTH STUDENT A & STUDENT B: Log into SMGR using the new password

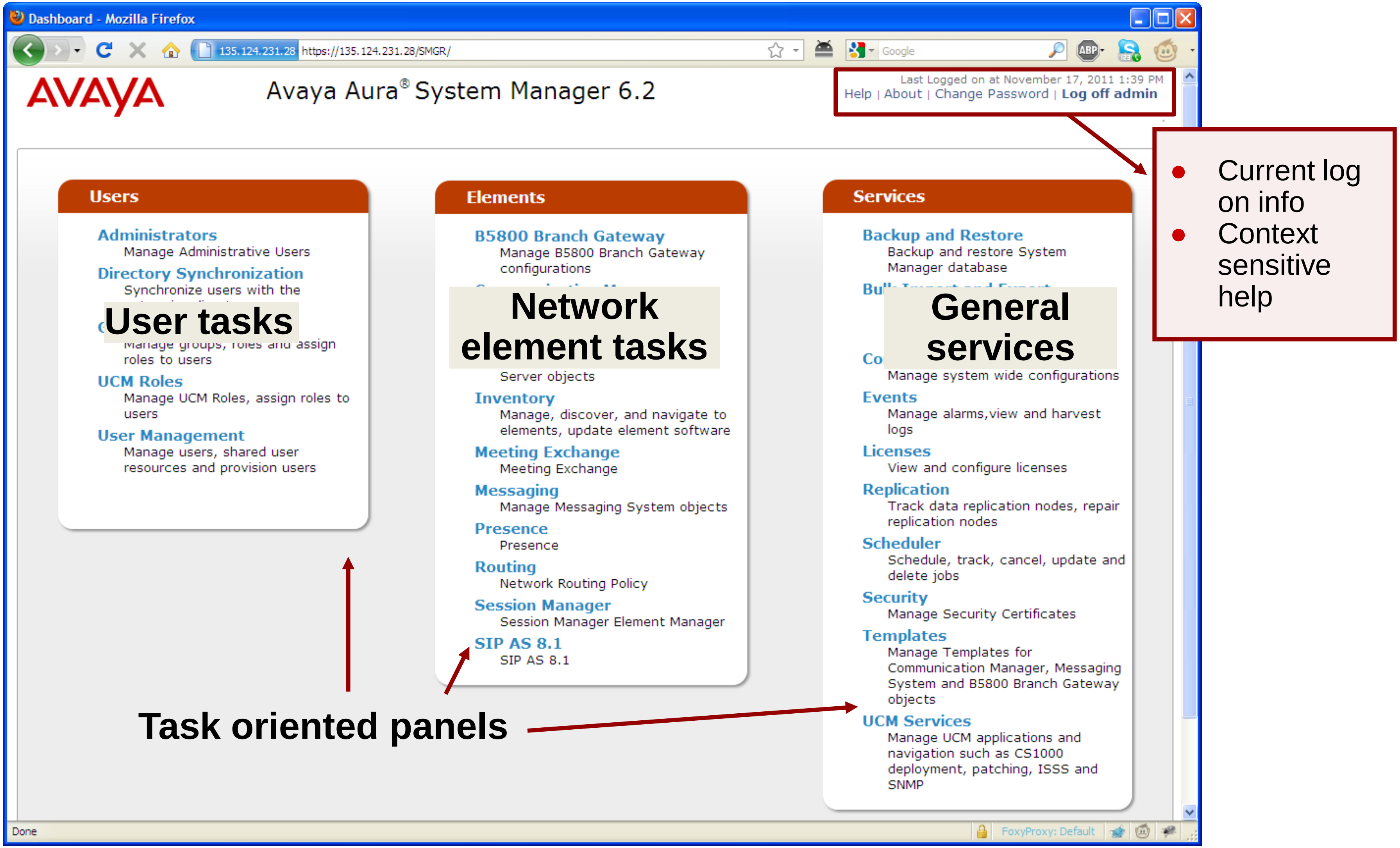
The keyboard layout on your remote desktop may not match your own! Be careful to ensure you enter the password correctly – Recommend type in notepad, then copy & paste?

Individual Exercise – both students



Student A Student B

System Manager Navigation: The SMGR Home Page



Dashboard - Mozilla Firefox
135.124.231.28 https://135.124.231.28/SMGR/
Google
Done
FoxyProxy: Default

AVAYA Avaya Aura® System Manager 6.2

Last Logged on at November 17, 2011 1:39 PM
Help | About | Change Password | Log off admin

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the

Manage groups, roles and assign roles to users

UCM Roles
Manage UCM Roles, assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway configurations

Server objects

Inventory
Manage, discover, and navigate to elements, update element software

Meeting Exchange
Meeting Exchange

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Co

Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

Scheduler
Schedule, track, cancel, update and delete jobs

Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway objects

UCM Services
Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

User tasks

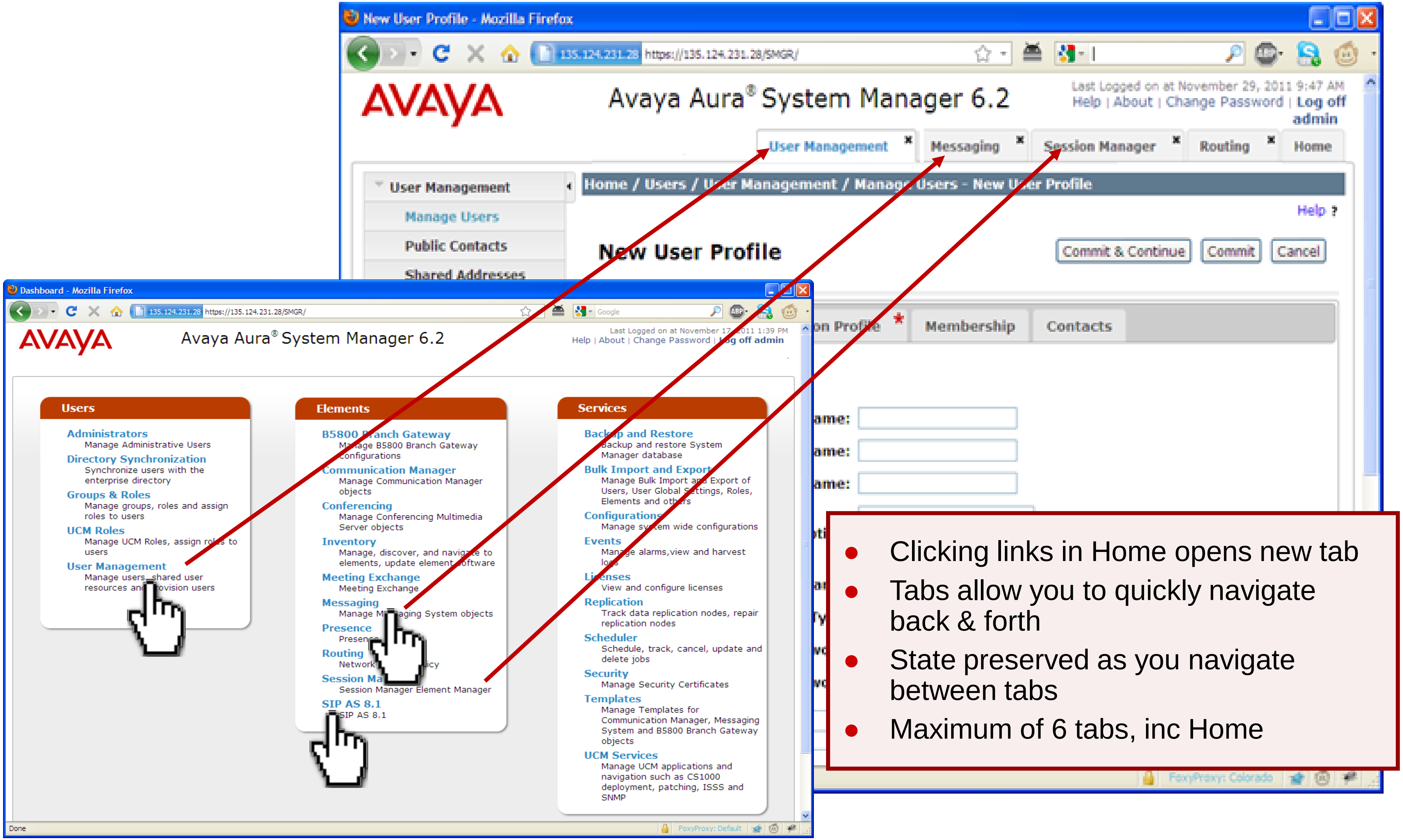
Network element tasks

General services

- Current log on info
- Context sensitive help

Task oriented panels

System Manager Navigation – Tabbed Browsing



New User Profile - Mozilla Firefox

https://135.124.231.28/SMGR/

Avaya Aura® System Manager 6.2

Last Logged on at November 29, 2011 9:47 AM
Help | About | Change Password | Log off admin

Home / Users / User Management / Manage Users - New User Profile

New User Profile

Dashboard - Mozilla Firefox

https://135.124.231.28/SMGR/

Avaya Aura® System Manager 6.2

Last Logged on at November 17, 2011 1:39 PM
Help | About | Change Password | Log off admin

Users

- Administrators — Manage Administrative Users
- Directory Synchronization — Synchronize users with the enterprise directory
- Groups & Roles — Manage groups, roles and assign roles to users
- UCM Roles — Manage UCM Roles, assign roles to users
- User Management — Manage users, shared user resources and provision users

Elements

- B5800 Branch Gateway — Manage B5800 Branch Gateway configurations
- Communication Manager — Manage Communication Manager objects
- Conferencing — Manage Conferencing Multimedia Server objects
- Inventory — Manage, discover, and navigate to elements, update element software
- Meeting Exchange — Meeting Exchange
- Messaging — Manage Messaging System objects
- Presence — Presence
- Routing — Network Routing Policy
- Session Manager — Session Manager Element Manager
- SIP AS 8.1 — SIP AS 8.1

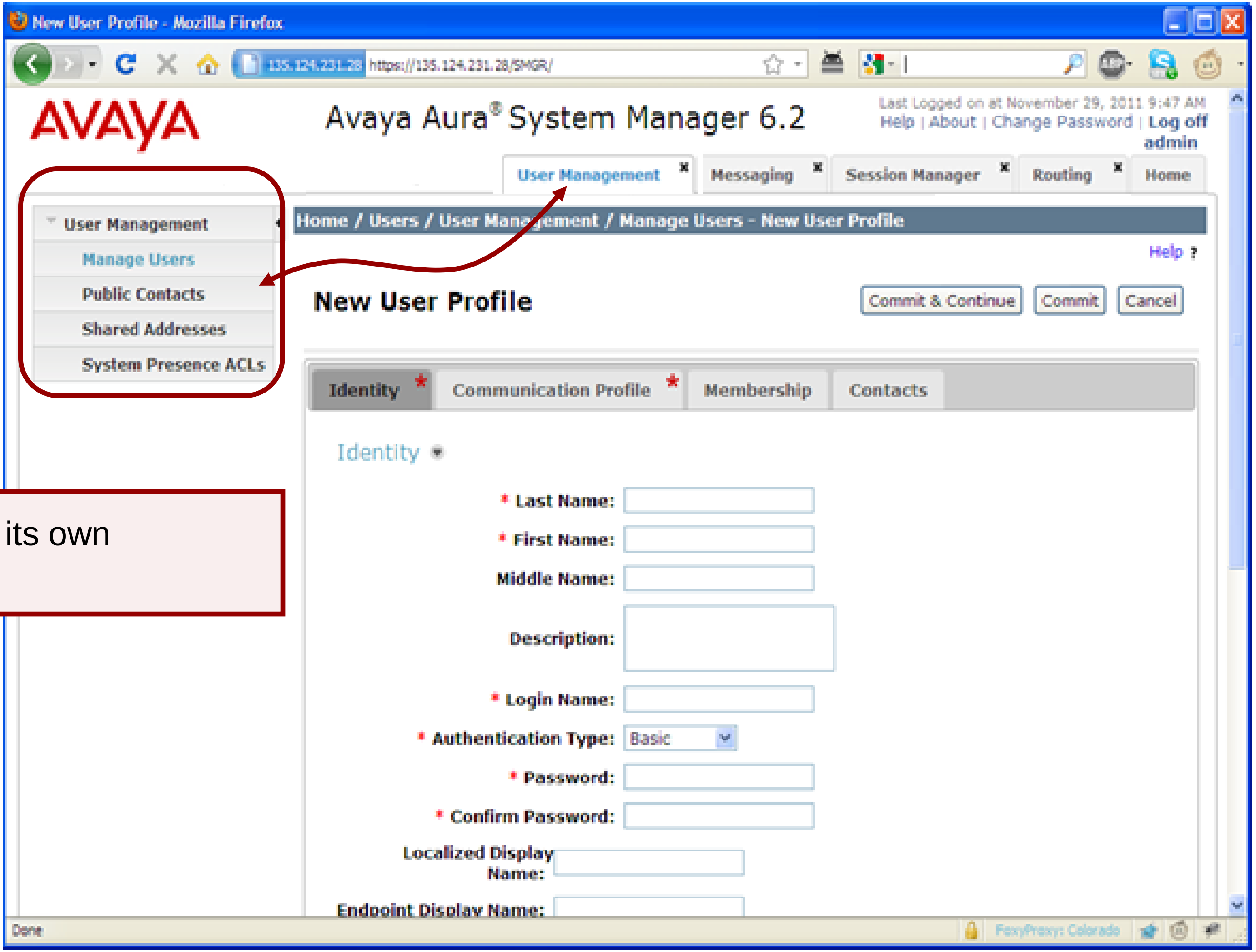
Services

- Backup and Restore — Backup and restore System Manager database
- Bulk Import and Export — Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others
- Configurations — Manage system wide configurations
- Events — Manage alarms,view and harvest logs
- Licenses — View and configure licenses
- Replication — Track data replication nodes, repair replication nodes
- Scheduler — Schedule, track, cancel, update and delete jobs
- Security — Manage Security Certificates
- Templates — Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway objects
- UCM Services — Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

Done

- Clicking links in Home opens new tab
- Tabs allow you to quickly navigate back & forth
- State preserved as you navigate between tabs
- Maximum of 6 tabs, inc Home

System Manager Navigation – Contextual Menus



New User Profile - Mozilla Firefox

https://135.124.231.28/SMGR/

Avaya Aura® System Manager 6.2

Last Logged on at November 29, 2011 9:47 AM

Help | About | Change Password | Log off admin

Home / Users / User Management / Manage Users - New User Profile

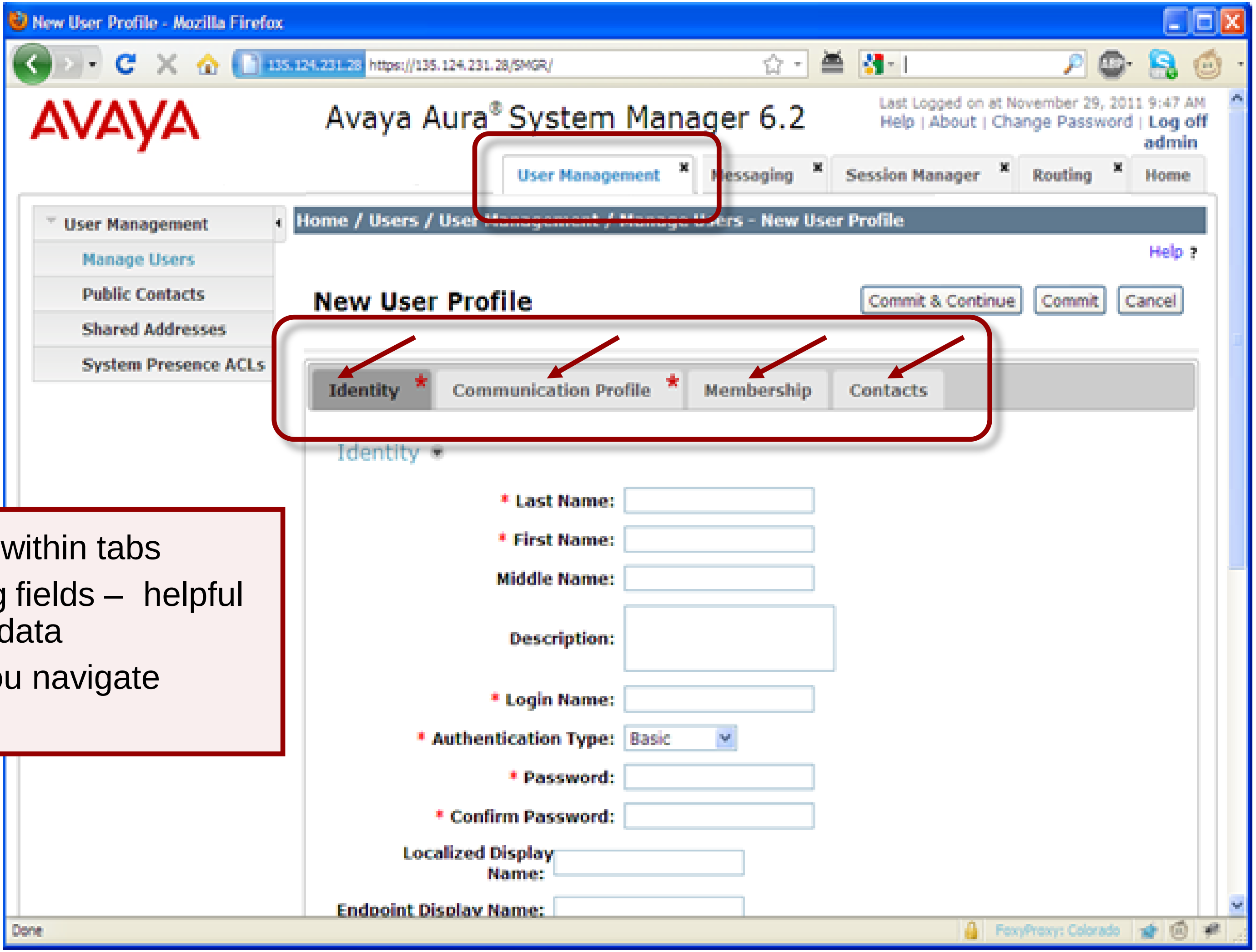
New User Profile

Identity

- * Last Name:
- * First Name:
- Middle Name:
- Description:
- * Login Name:
- * Authentication Type: Basic
- * Password:
- * Confirm Password:
- Localized Display Name:
- Endpoint Display Name:

- Each subject Tab has its own contextual menu

System Manager Navigation – Tabs within Tabs



New User Profile - Mozilla Firefox

https://135.124.231.28/SMGR/

Avaya Aura® System Manager 6.2

Last Logged on at November 29, 2011 9:47 AM
Help | About | Change Password | Log off admin

Home / Users / User Management / Manage Users - New User Profile

New User Profile

Identity

* Last Name:

* First Name:

Middle Name:

Description:

* Login Name:

* Authentication Type: Basic

* Password:

* Confirm Password:

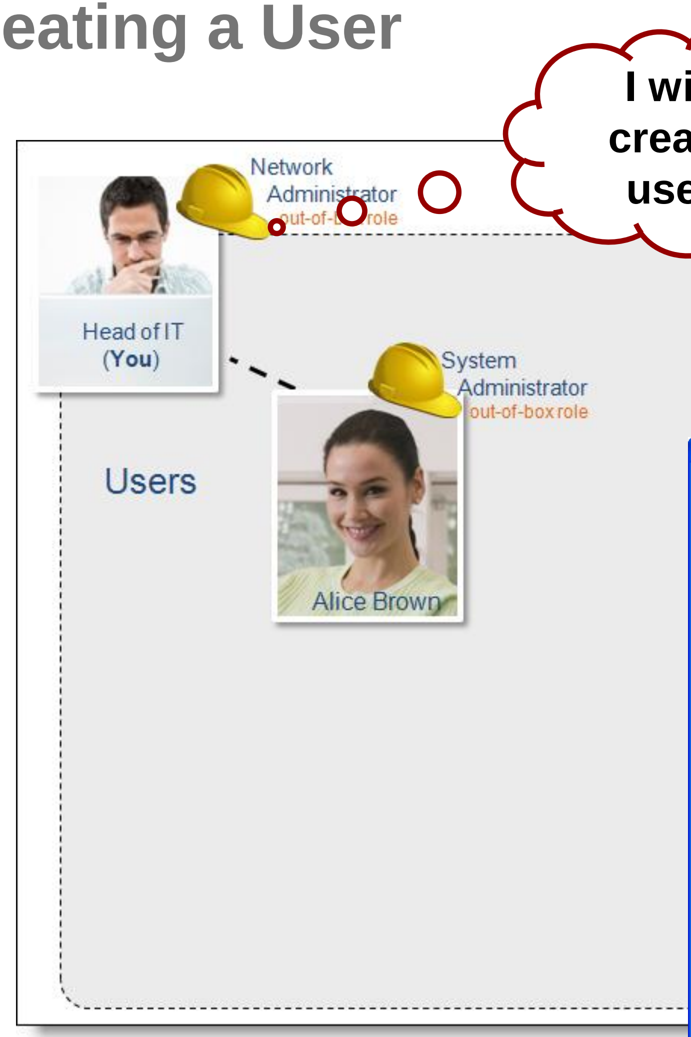
Localized Display Name:

Endpoint Display Name:

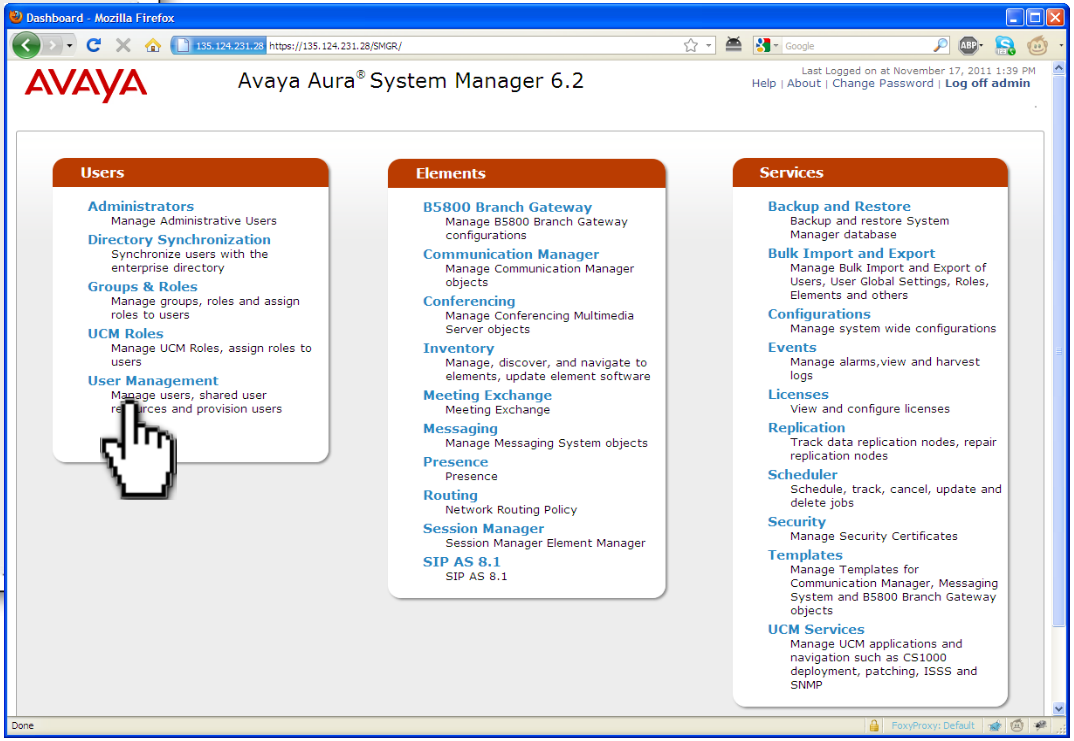
Some screens have tabs within tabs

- Helps with negotiating fields – helpful when there is a lot of data
- State preserved as you navigate between tabs

Creating a User


I will create user
Network Administrator out-of-box role
Head of IT (You)
System Administrator out-of-box role
Users
Alice Brown

Click User Management from Home page


Dashboard - Mozilla Firefox
135.124.231.28 https://135.124.231.28/SMGR/
Google
AVAYA
Done
FoxyProxy: Default

Avaya Aura® System Manager 6.2

Last Logged on at November 17, 2011 1:39 PM
Help | About | Change Password | Log off admin

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

UCM Roles
Manage UCM Roles, assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway configurations

Communication Manager
Manage Communication Manager objects

Conferencing
Manage Conferencing Multimedia Server objects

Inventory
Manage, discover, and navigate to elements, update element software

Meeting Exchange
Meeting Exchange

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

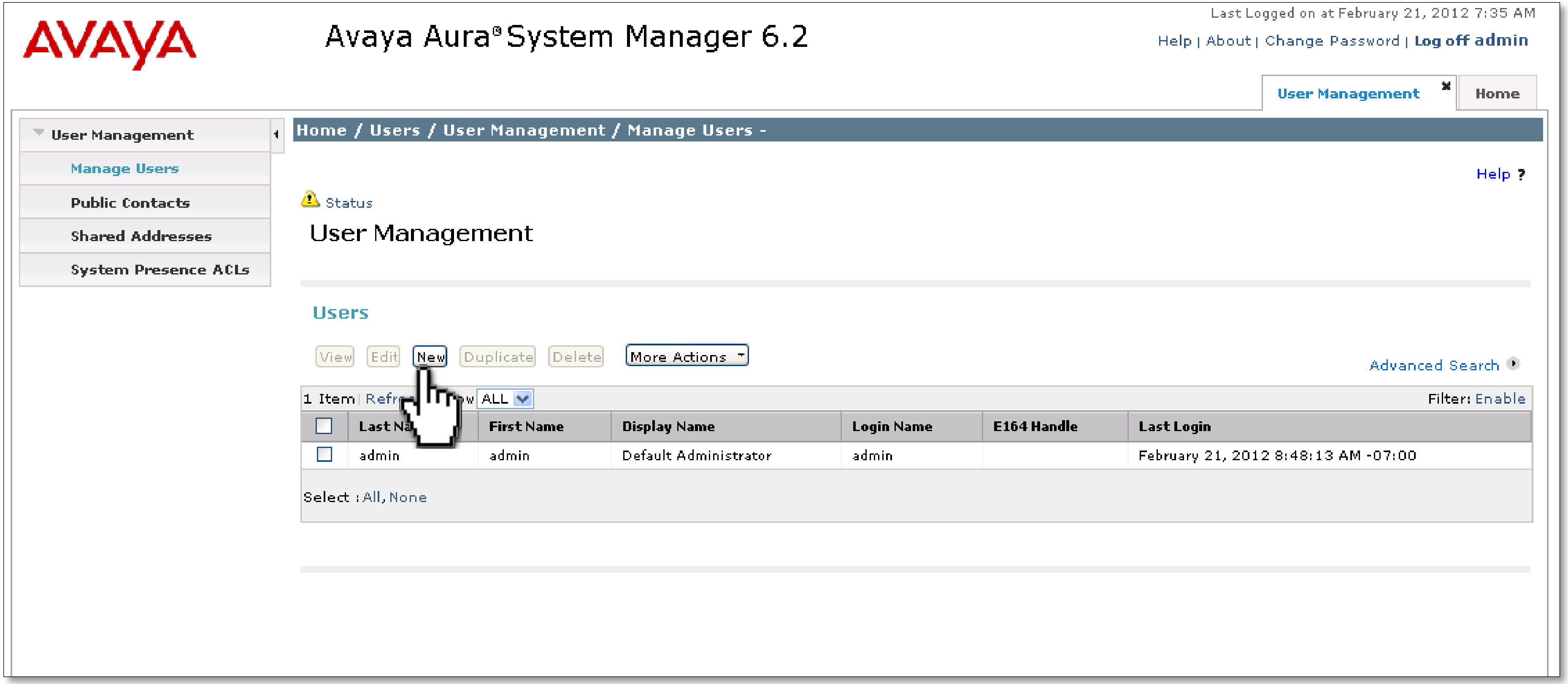
Scheduler
Schedule, track, cancel, update and delete jobs

Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway objects

UCM Services
Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

Creating a User (continued)



Last Logged on at February 21, 2012 7:35 AM

Avaya Aura® System Manager 6.2

Help | About | Change Password | Log off admin

Home / Users / User Management / Manage Users -

User Management

Users

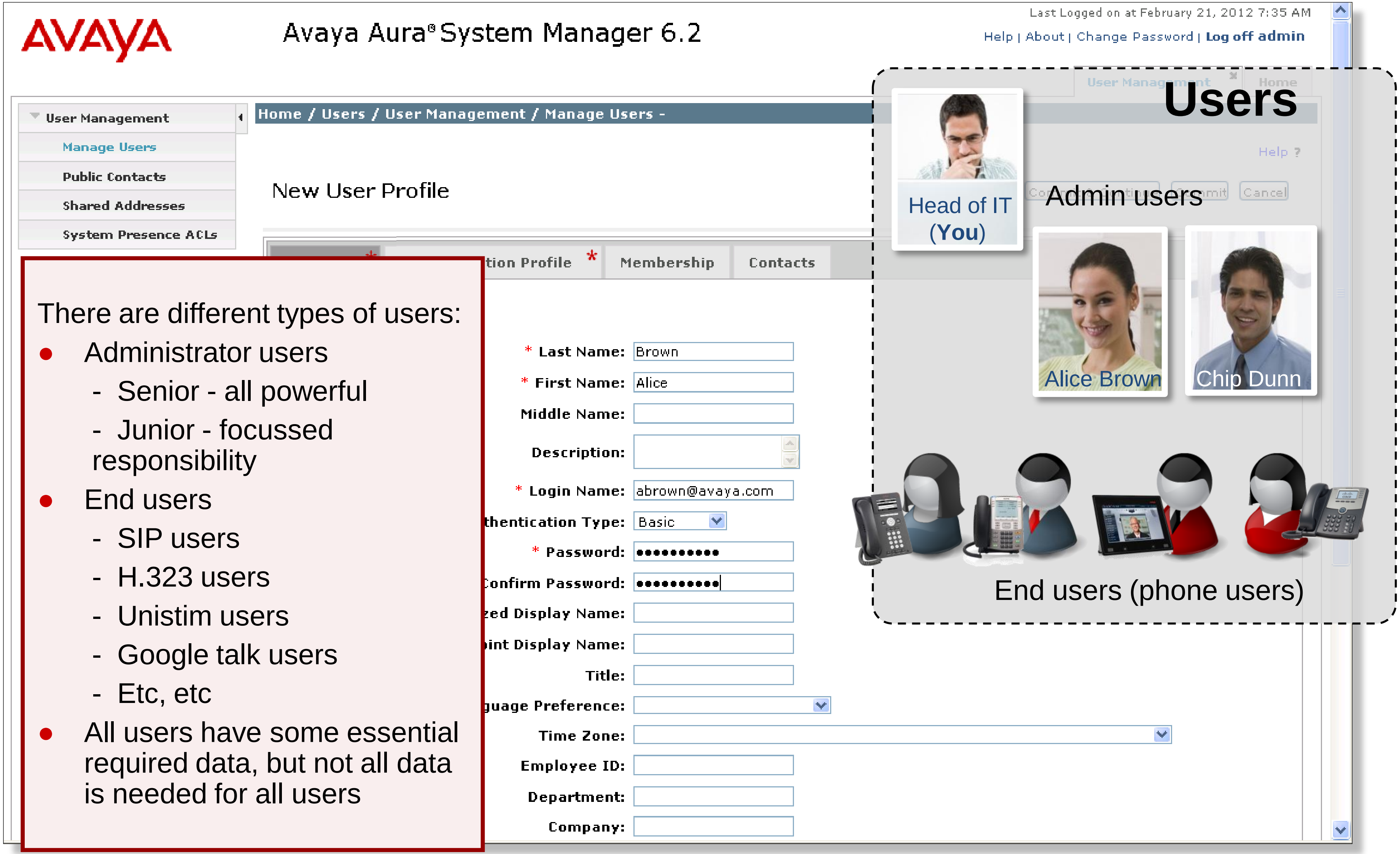
1 Item | Refresh | Show ALL | Filter: Enable

□	Last Name	First Name	Display Name	Login Name	E164 Handle	Last Login
□	admin	admin	Default Administrator	admin		February 21, 2012 8:48:13 AM -07:00

Select : All, None

- To begin with there will be only one user – the default *admin* user.
- Click ‘New’ to create a user.

Users: Different Types



Avaya Aura® System Manager 6.2

Last Logged on at February 21, 2012 7:35 AM

Help | About | Change Password | Log off admin

Home / Users / User Management / Manage Users -

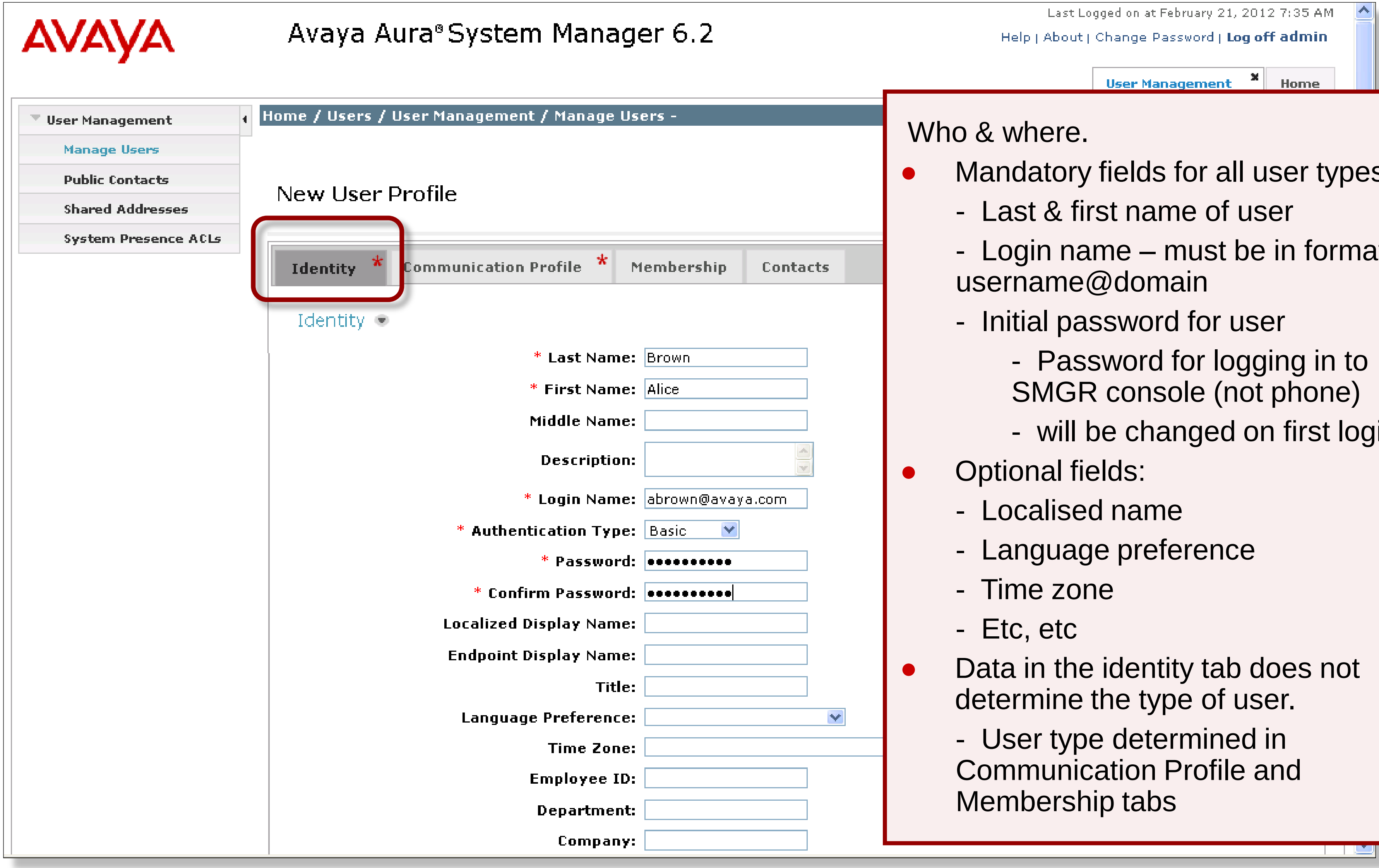
New User Profile

* Last Name:	Brown
* First Name:	Alice
Middle Name:	
Description:	
* Login Name:	abrown@avaya.com
thentication Type:	Basic
* Password:	●●●●●●●●●●
onfirm Password:	●●●●●●●●●●
zed Display Name:	
int Display Name:	
Title:	
uage Preference:	
Time Zone:	
Employee ID:	
Department:	
Company:	

There are different types of users:

- Administrator users
  - Senior - all powerful
  - Junior - focussed responsibility
- End users
  - SIP users
  - H.323 users
  - Unistim users
  - Google talk users
  - Etc, etc
- All users have some essential required data, but not all data is needed for all users

Users: User Identity – Identity Tab


AVAYA
Avaya Aura® System Manager 6.2
Last Logged on at February 21, 2012 7:35 AM
Help | About | Change Password | Log off admin
User Management
Home
User Management
Manage Users
Public Contacts
Shared Addresses
System Presence ACLs
Home / Users / User Management / Manage Users -
Identity *
Communication Profile *
Membership
Contacts

New User Profile

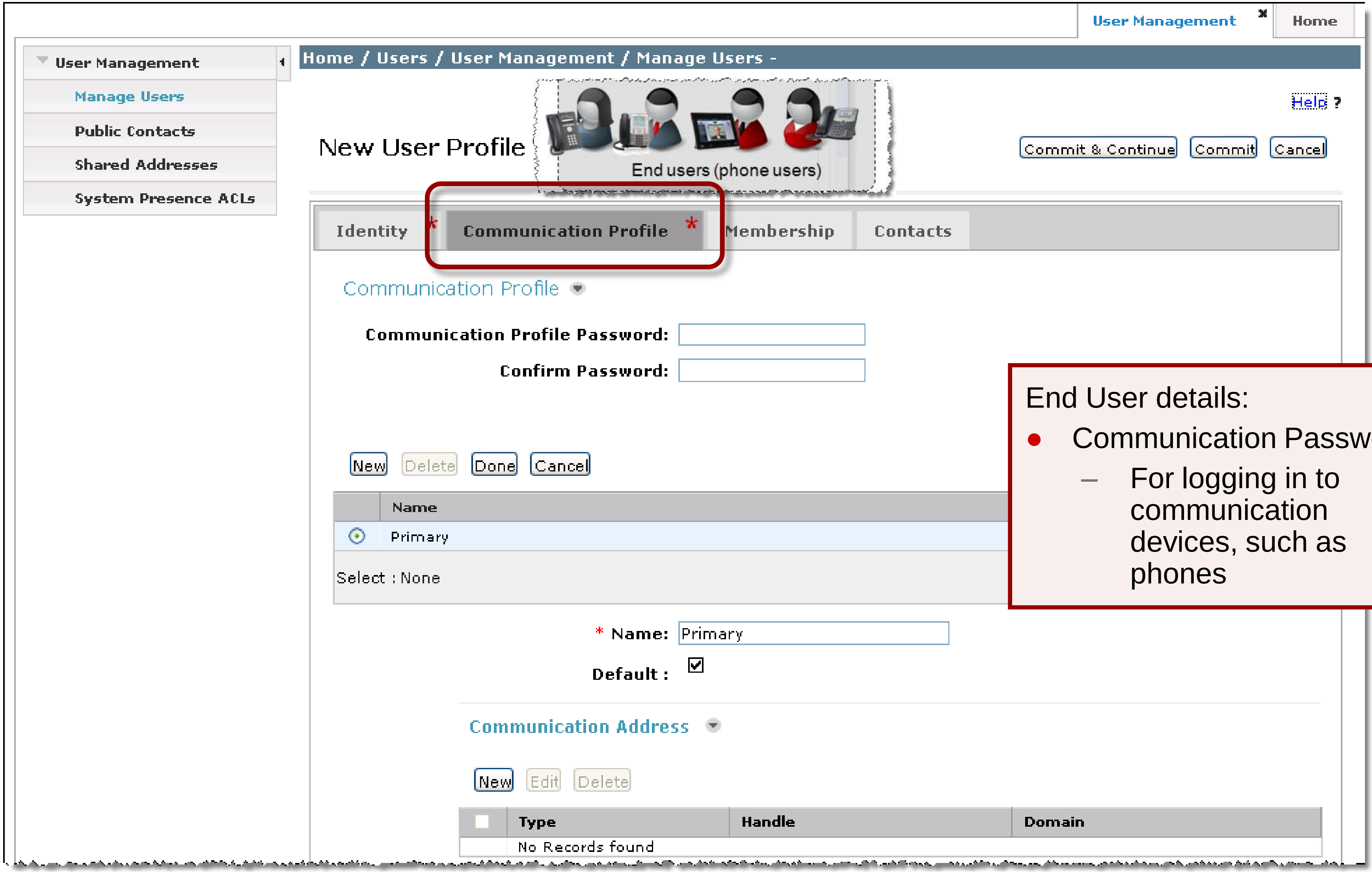
Identity

* Last Name:	Brown
* First Name:	Alice
Middle Name:	
Description:	
* Login Name:	abrown@avaya.com
* Authentication Type:	Basic
* Password:	●●●●●●●●●●●
* Confirm Password:	●●●●●●●●●●●
Localized Display Name:	
Endpoint Display Name:	
Title:	
Language Preference:	
Time Zone:	
Employee ID:	
Department:	
Company:	

Who & where.

- Mandatory fields for all user types:
  - Last & first name of user
  - Login name – must be in format username@domain
  - Initial password for user
    - Password for logging in to SMGR console (not phone)
    - will be changed on first login
- Optional fields:
  - Localised name
  - Language preference
  - Time zone
  - Etc, etc
- Data in the identity tab does not determine the type of user.
  - User type determined in Communication Profile and Membership tabs

Users: End User Profiles – Communication Profiles Tab



New User Profile

Communication Profile

Communication Profile Password:

Confirm Password:

	Name
●	Primary

Select : None

* Name: Primary

Default : ☑

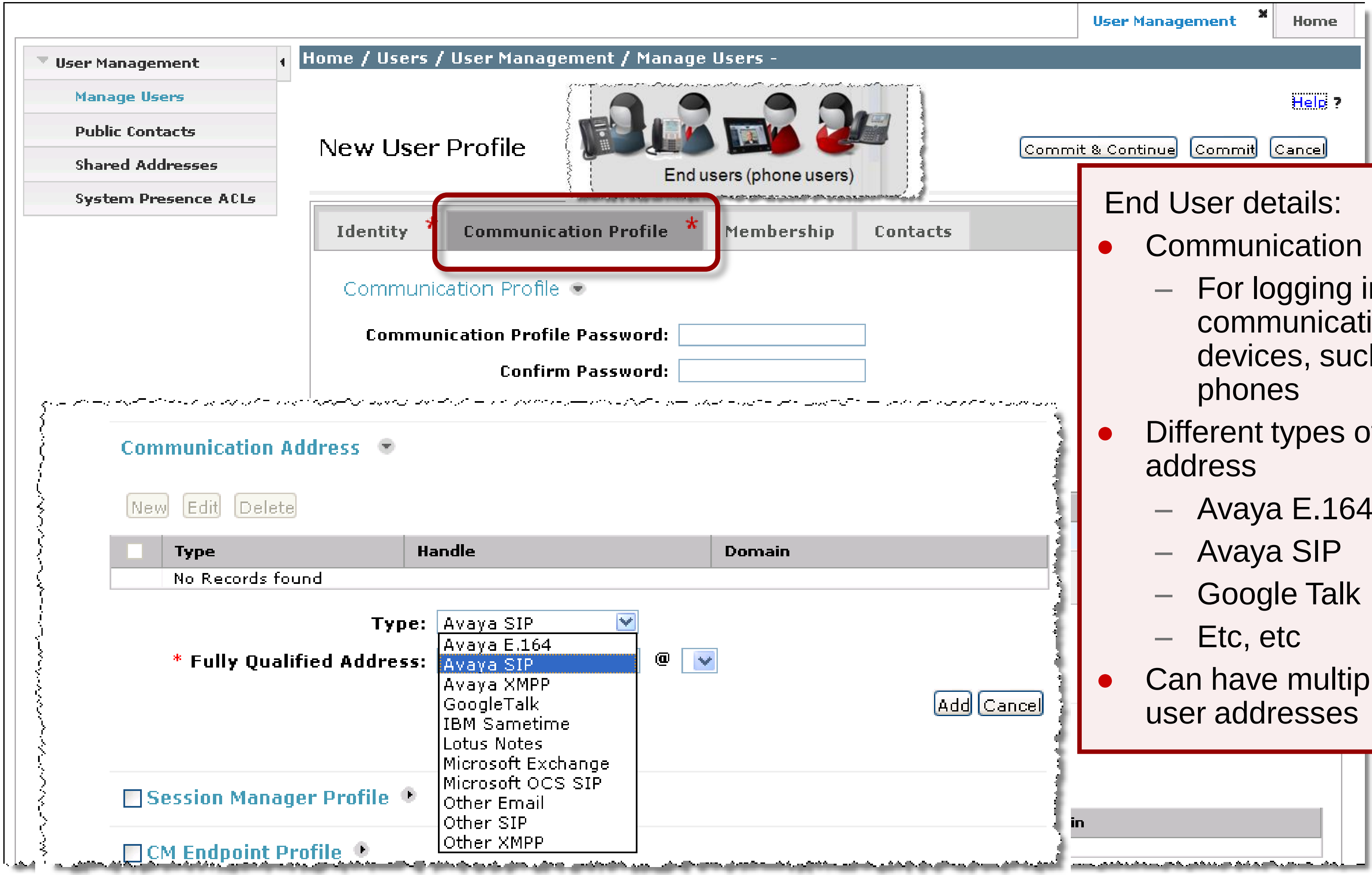
Communication Address

□	Type	Handle	Domain
	No Records found		

End User details:

- Communication Password
  - For logging in to communication devices, such as phones

Users: End User Profiles – Communication Profiles Tab (continued)



New User Profile

Communication Profile

Communication Profile Password:

Confirm Password:

Communication Address

□	Type	Handle	Domain
	No Records found		

Type: Avaya SIP

- Avaya E.164
- Avaya SIP
- Avaya XMPP
- GoogleTalk
- IBM Sametime
- Lotus Notes
- Microsoft Exchange
- Microsoft OCS SIP
- Other Email
- Other SIP
- Other XMPP

* Fully Qualified Address: @

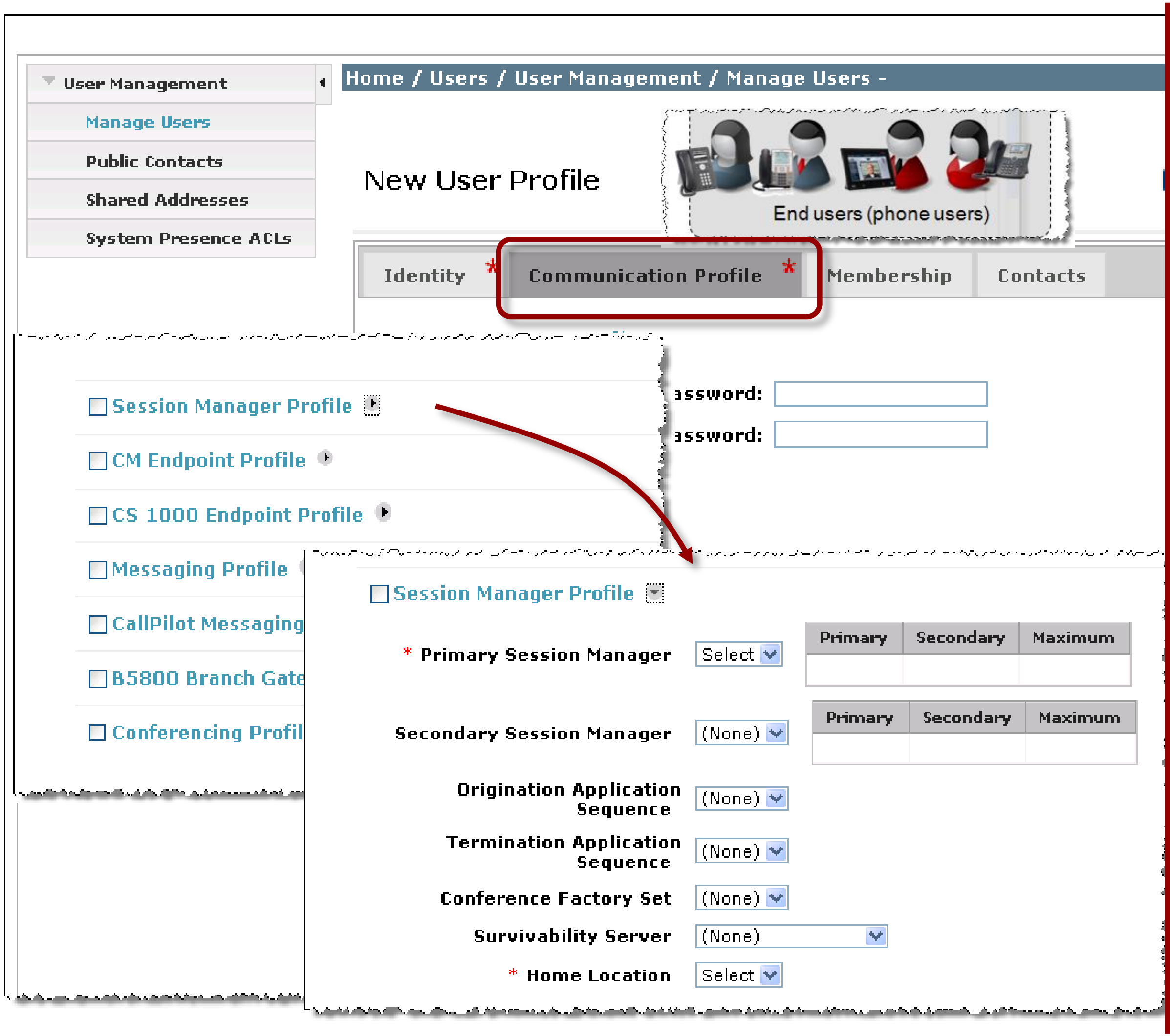
□ Session Manager Profile

□ CM Endpoint Profile

End User details:

- Communication Password
  - For logging in to communication devices, such as phones
- Different types of end-user address
  - Avaya E.164
  - Avaya SIP
  - Google Talk
  - Etc, etc
- Can have multiple end-user addresses

Users: End User Profiles – Communication Profiles Tab (continued)



assword:

assword:

- □ Session Manager Profile
- □ CM Endpoint Profile
- □ CS 1000 Endpoint Profile
- □ Messaging Profile
- □ CallPilot Messaging
- □ B5800 Branch Gate
- □ Conferencing Profil

□ Session Manager Profile

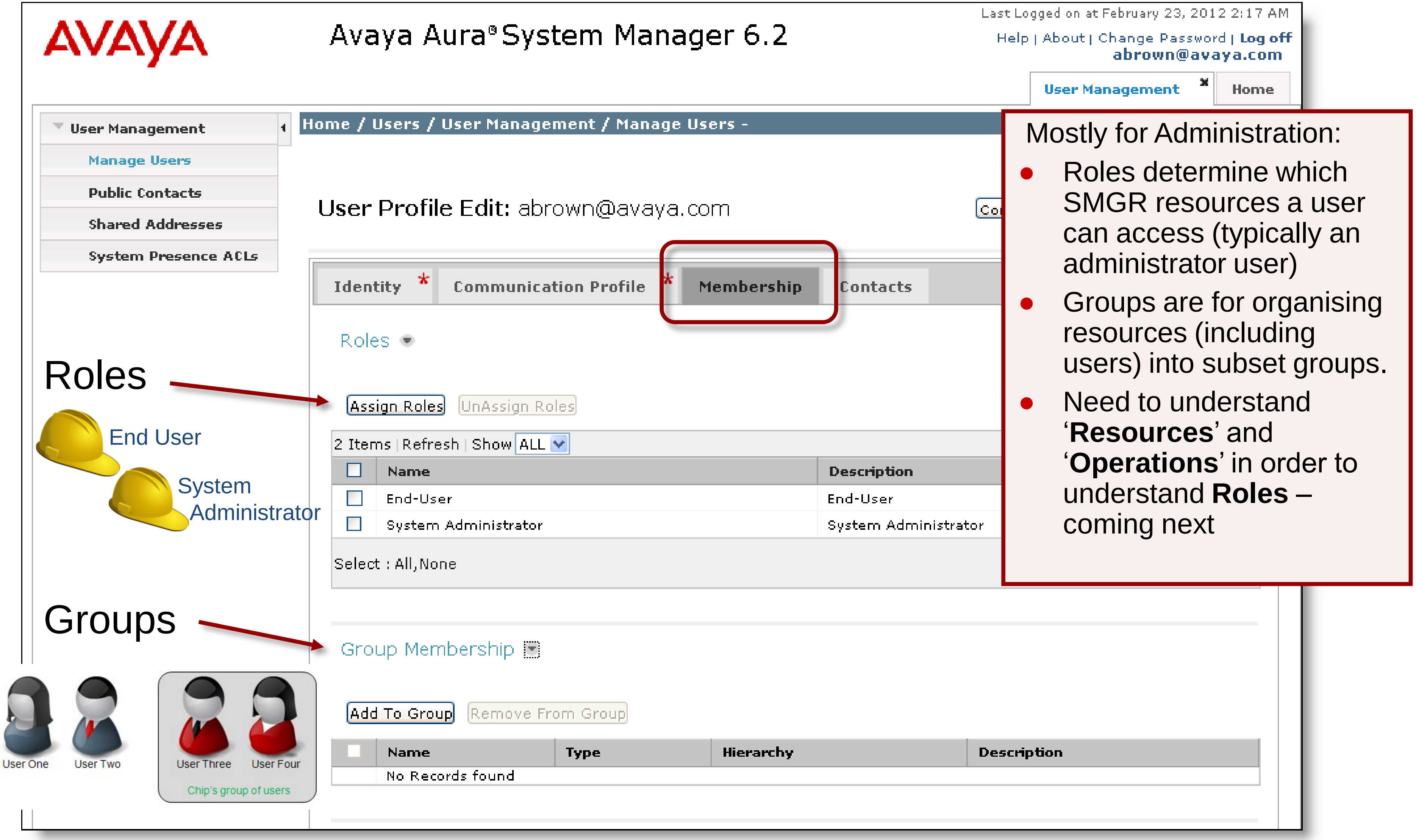
		Primary	Secondary	Maximum
* Primary Session Manager	Select			
Secondary Session Manager	(None)			

Origination Application Sequence	(None)
Termination Application Sequence	(None)
Conference Factory Set	(None)
Survivability Server	(None)
* Home Location	Select

End User details:

- Communication Password
  - For logging in to communication devices, such as phones
- Different types of end-user address
  - Avaya E.164
  - Avaya SIP
  - Google Talk
  - Etc, etc
- Can have multiple end-user addresses
- There are currently 7 types of communication profile
  - Each opens to reveal specific server & service settings
  - Users can have all, some or none of these profiles
- Covered in other dedicated courses

Users: Roles & Groups – Membership Tab



Avaya Aura® System Manager 6.2

Last Logged on at February 23, 2012 2:17 AM

Help | About | Change Password | Log off

abrown@avaya.com

Home / Users / User Management / Manage Users -

User Profile Edit: abrown@avaya.com

Roles

2 Items | Refresh | Show ALL

☐	Name	Description
☐	End-User	End-User
☐	System Administrator	System Administrator

Select : All, None

Group Membership

☐	Name	Type	Hierarchy	Description
	No Records found			

Roles

Groups

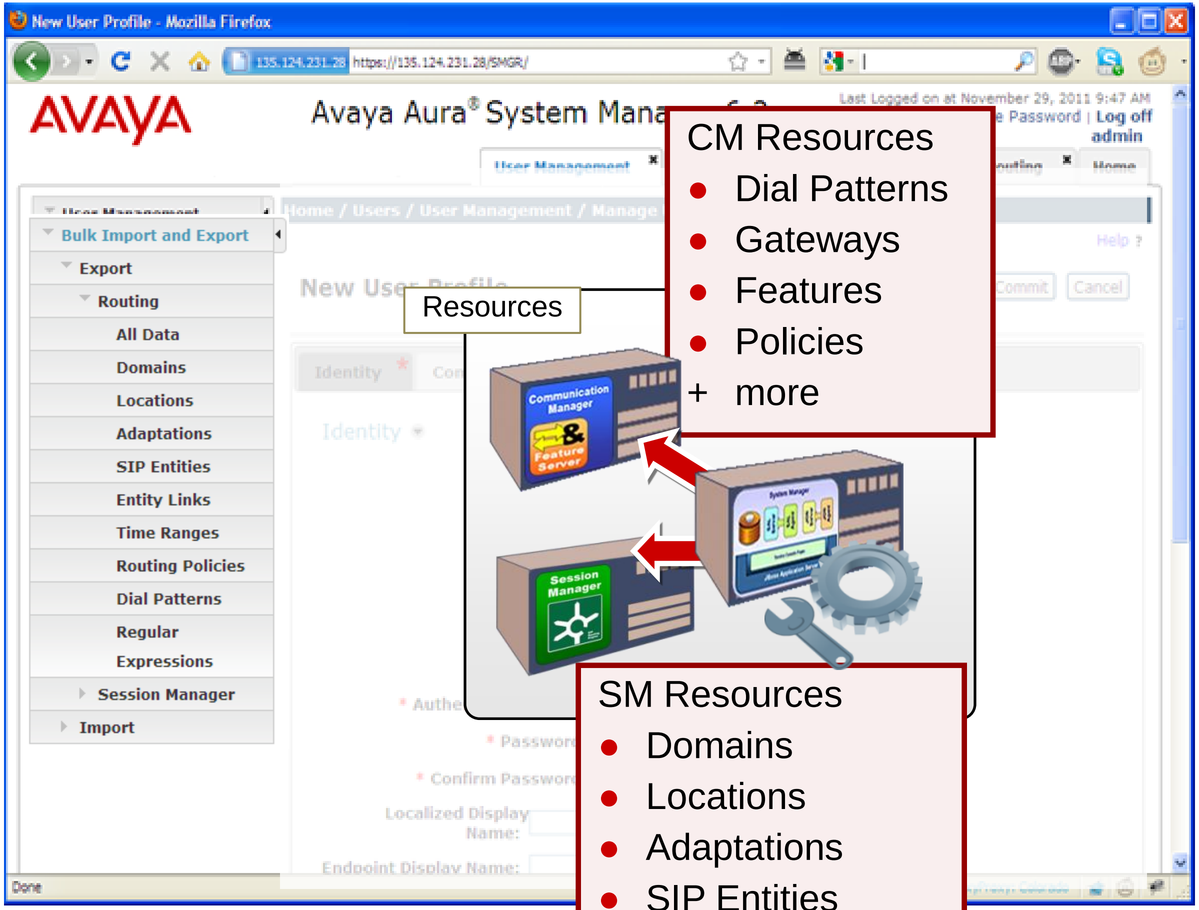
Mostly for Administration:

- Roles determine which SMGR resources a user can access (typically an administrator user)
- Groups are for organising resources (including users) into subset groups.
- Need to understand ‘**Resources**’ and ‘**Operations**’ in order to understand **Roles** – coming next

SMGR Resources & Operations

What is a resource?

- Anything administered with SMGR
- Some resources will be product specific.
  - SM resources
  - CM resources
- Others will be cross platform
  - User management tools
  - System tools (backup/restore, etc)



New User Profile - Mozilla Firefox

135.124.231.28 https://135.124.231.28/SMGR/

AVAYA Avaya Aura® System Mana

Last Logged on at November 29, 2011 9:47 AM

Password | Log off admin

CM Resources

- Dial Patterns
- Gateways
- Features
- Policies
- + more

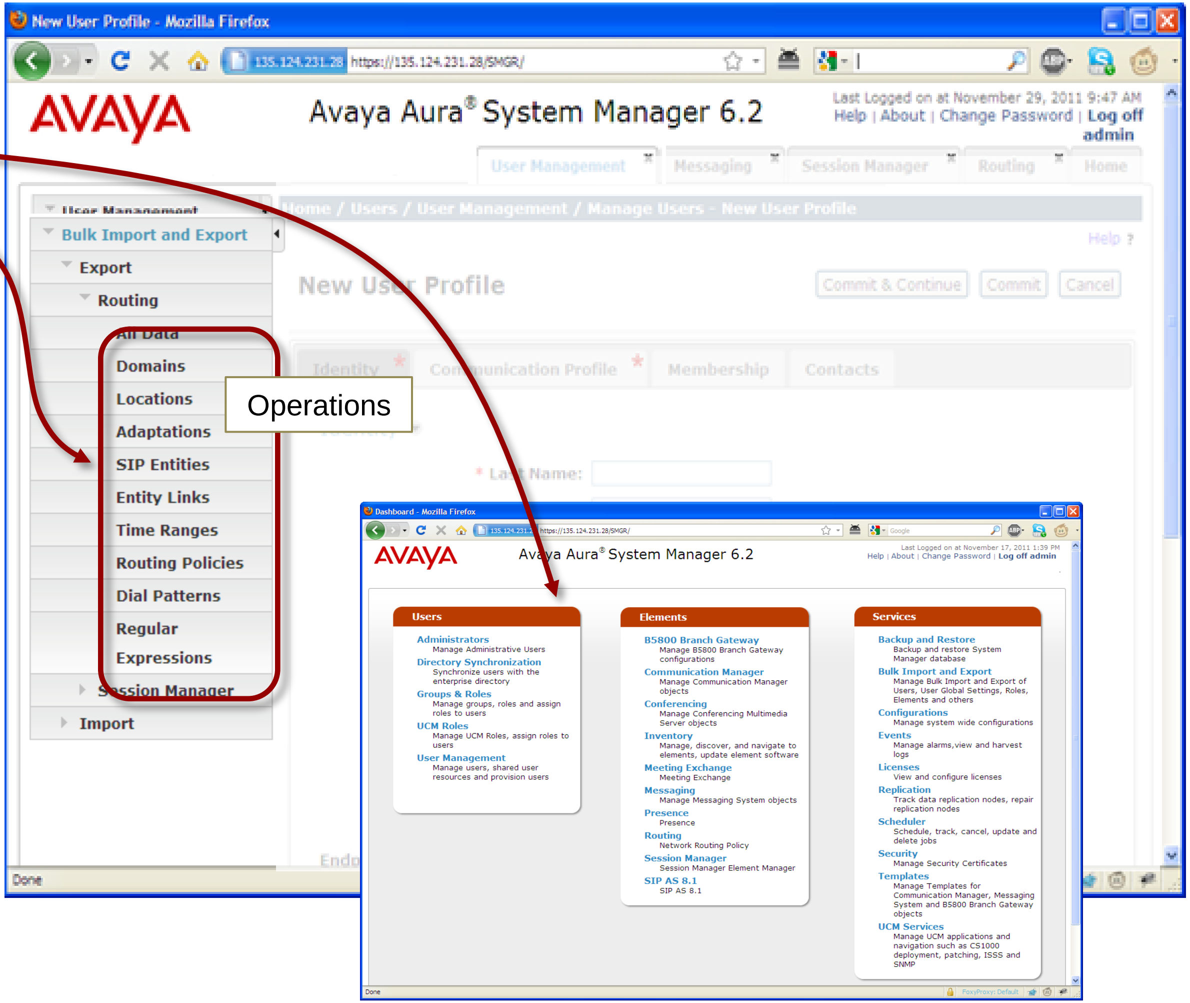
SM Resources

- Domains
- Locations
- Adaptations
- SIP Entities
- + more

SMGR Resources & Operations (continued)

What is an Operation?

- Anything on a SMGR menu
- Provides access to perform an action on a resource



Users

- Administrators: Manage Administrative Users
- Directory Synchronization: Synchronize users with the enterprise directory
- Groups & Roles: Manage groups, roles and assign roles to users
- UCM Roles: Manage UCM Roles, assign roles to users
- User Management: Manage users, shared user resources and provision users

Elements

- B5800 Branch Gateway: Manage B5800 Branch Gateway configurations
- Communication Manager: Manage Communication Manager objects
- Conferencing: Manage Conferencing Multimedia Server objects
- Inventory: Manage, discover, and navigate to elements, update element software
- Meeting Exchange: Meeting Exchange
- Messaging: Manage Messaging System objects
- Presence: Presence
- Routing: Network Routing Policy
- Session Manager: Session Manager Element Manager
- SIP AS 8.1: SIP AS 8.1

Services

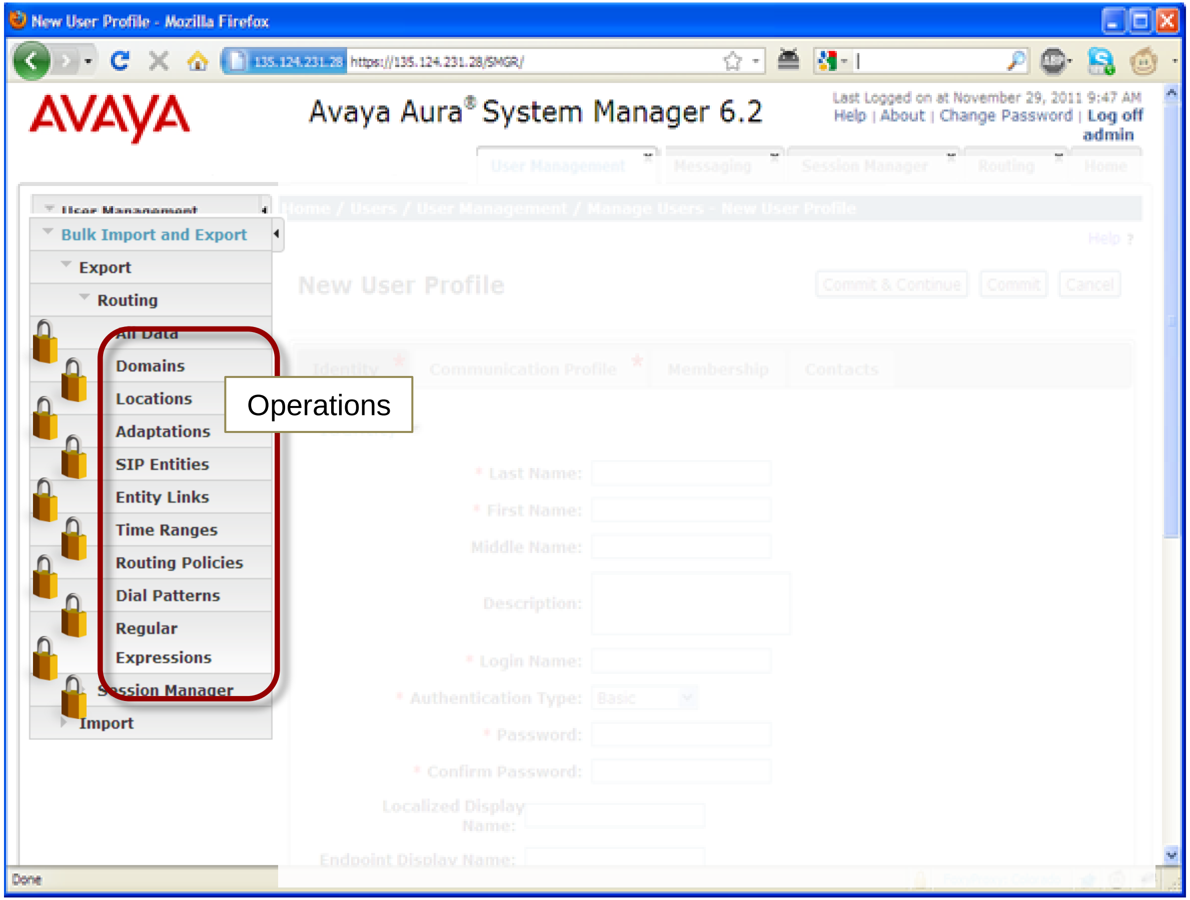
- Backup and Restore: Backup and restore System Manager database
- Bulk Import and Export: Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others
- Configurations: Manage system wide configurations
- Events: Manage alarms,view and harvest logs
- Licenses: View and configure licenses
- Replication: Track data replication nodes, repair replication nodes
- Scheduler: Schedule, track, cancel, update and delete jobs
- Security: Manage Security Certificates
- Templates: Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway objects
- UCM Services: Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

Operations are Combined & Made Accessible through Roles

- By default all operations are locked
- A user needs permission (keys) to access a resource
- Permissions are combined in Roles

- Roles are then assigned to users

System Administrator



New User Profile - Mozilla Firefox

135.124.231.28 https://135.124.231.28/SMGR/

AVAYA

Avaya Aura® System Manager 6.2

Last Logged on at November 29, 2011 9:47 AM
Help | About | Change Password | **Log off admin**

User Management | Messaging | Session Manager | Routing | Home

- User Management
- Bulk Import and Export
  - Export
    - Routing
      - All Data
      - Domains
      - Locations
      - Adaptations
      - SIP Entities
      - Entity Links
      - Time Ranges
      - Routing Policies
      - Dial Patterns
      - Regular Expressions
    - Session Manager
  - Import

Home / Users / User Management / Manage Users - New User Profile

Help ?

New User Profile

Commit & Continue | Commit | Cancel

Identity * | Communication Profile * | Membership | Contacts

* Last Name:

* First Name:

Middle Name:

Description:

* Login Name:

* Authentication Type: Basic

* Password:

* Confirm Password:

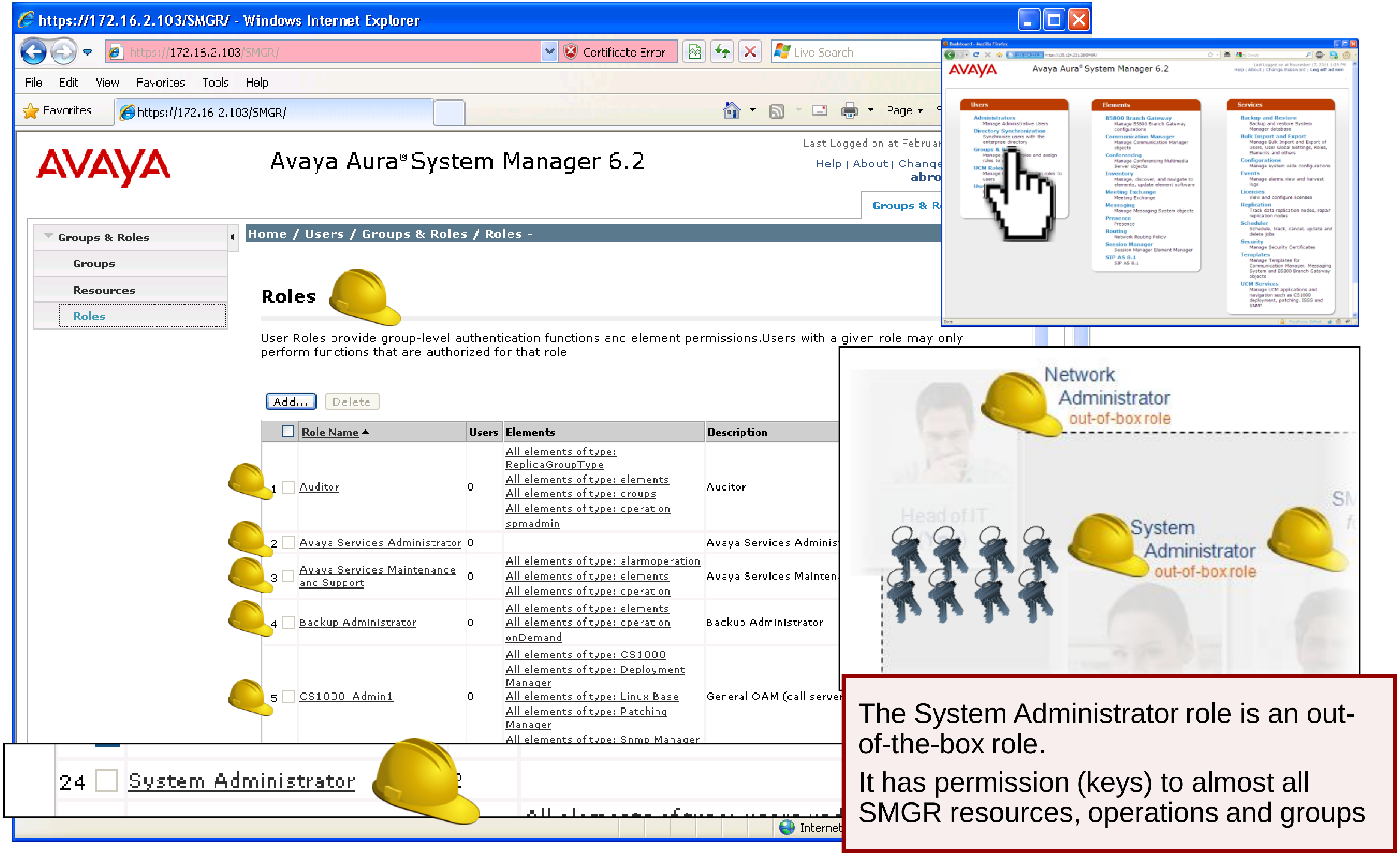
Localized Display Name:

Endpoint Display Name:

Done

Operations

SMGR Roles: Out-of-the-Box Roles


https://172.16.2.103/SMGR/ - Windows Internet Explorer
https://172.16.2.103/SMGR/
Certificate Error
Live Search
File Edit View Favorites Tools Help
Favorites
https://172.16.2.103/SMGR/
Page
AVAYA
Avaya Aura® System Manager 6.2
Last Logged on at Februar
Help | About | Change
abro
Groups & R
Groups & Roles
Groups
Resources
Roles
Home / Users / Groups & Roles / Roles -
Add...
Delete
Internet

Roles

User Roles provide group-level authentication functions and element permissions.Users with a given role may only perform functions that are authorized for that role

□	Role Name ▲	Users	Elements	Description
1 □	Auditor	0	All elements of type: ReplicaGroupType All elements of type: elements All elements of type: groups All elements of type: operation spmadmin	Auditor
2 □	Avaya Services Administrator	0		Avaya Services Adminis
3 □	Avaya Services Maintenance and Support	0	All elements of type: alarmoperation All elements of type: elements All elements of type: operation	Avaya Services Mainten
4 □	Backup Administrator	0	All elements of type: elements All elements of type: operation onDemand	Backup Administrator
5 □	CS1000_Admin1	0	All elements of type: CS1000 All elements of type: Deployment Manager All elements of type: Linux Base All elements of type: Patching Manager All elements of type: Snmp Manager	General OAM (call server
24 □	System Administrator	2	All elements of type:	

Dashboard - Mozilla Firefox
https://135.124.231.28/SMGR/
Google
AVAYA
Avaya Aura® System Manager 6.2
Last Logged on at November 17, 2011 1:39 PM
Help | About | Change Password | Log off admin
Done
FoxyProxy: Default

Users
- Administrators: Manage Administrative Users
- Directory Synchronization: Synchronize users with the enterprise directory
- Groups & R: Manage roles and assign roles to u
- UCM Roles: Manage roles to users
- Use

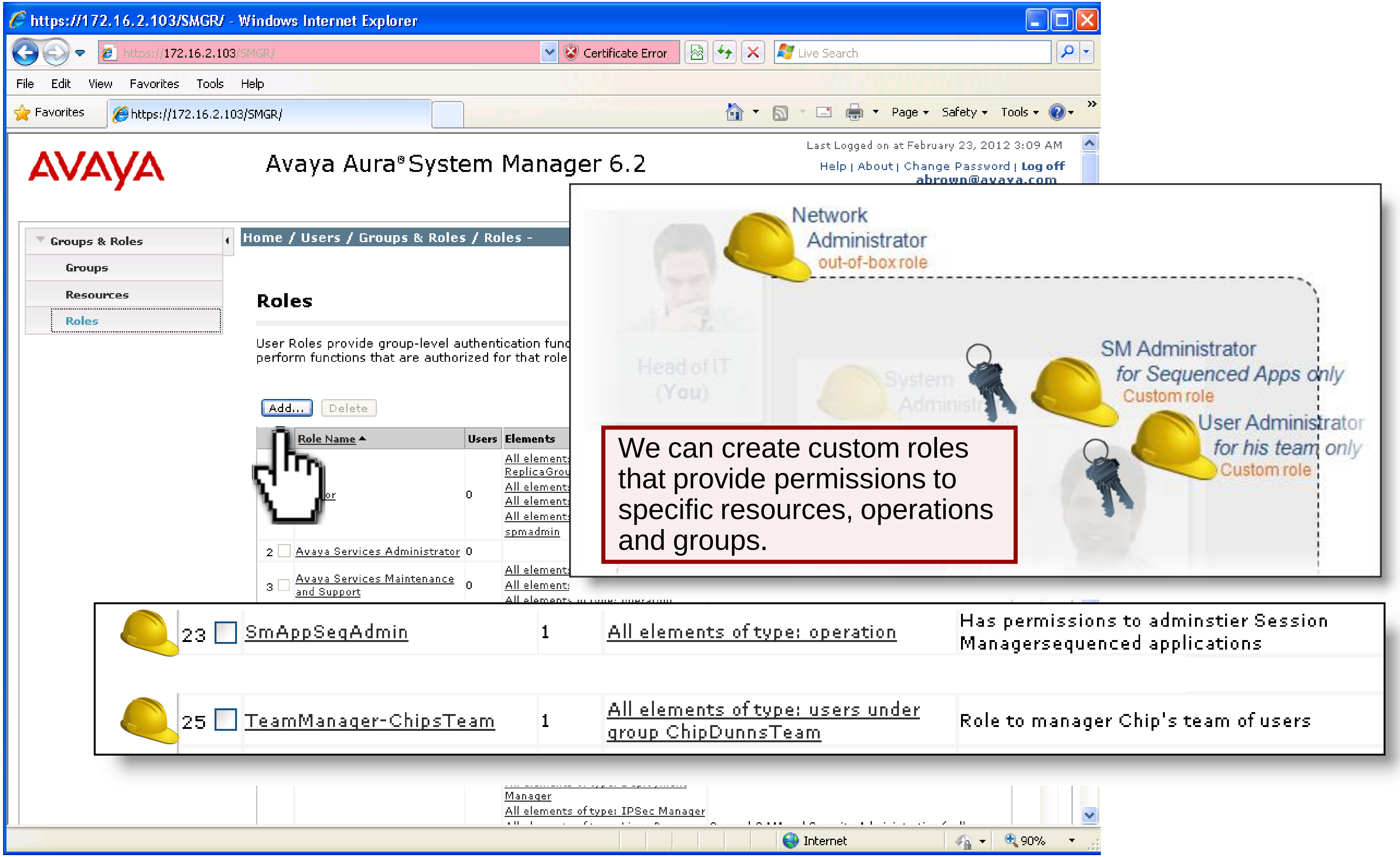
Elements
- B5800 Branch Gateway: Manage B5800 Branch Gateway configurations
- Communication Manager: Manage Communication Manager objects
- Conferencing: Manage Conferencing Multimedia Server objects
- Inventory: Manage, discover, and navigate to elements, update element software
- Meeting Exchange: Meeting Exchange
- Messaging: Manage Messaging System objects
- Presence: Presence
- Routing: Network Routing Policy
- Session Manager: Session Manager Element Manager
- SIP AS 8.1: SIP AS 8.1

Services
- Backup and Restore: Backup and restore System Manager database
- Bulk Import and Export: Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others
- Configurations: Manage system wide configurations
- Events: Manage alarms,view and harvest logs
- Licenses: View and configure licenses
- Replication: Track data replication nodes, repair replication nodes
- Scheduler: Schedule, track, cancel, update and delete jobs
- Security: Manage Security Certificates
- Templates: Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway objects
- UCM Services: Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

The System Administrator role is an out-of-the-box role.

It has permission (keys) to almost all SMGR resources, operations and groups

SMGR Roles: Custom Roles



https://172.16.2.103/SMGR/ - Windows Internet Explorer

Avaya Aura® System Manager 6.2

Last Logged on at February 23, 2012 3:09 AM

Help | About | Change Password | Log off

abrown@avaya.com

Home / Users / Groups & Roles / Roles -

Roles

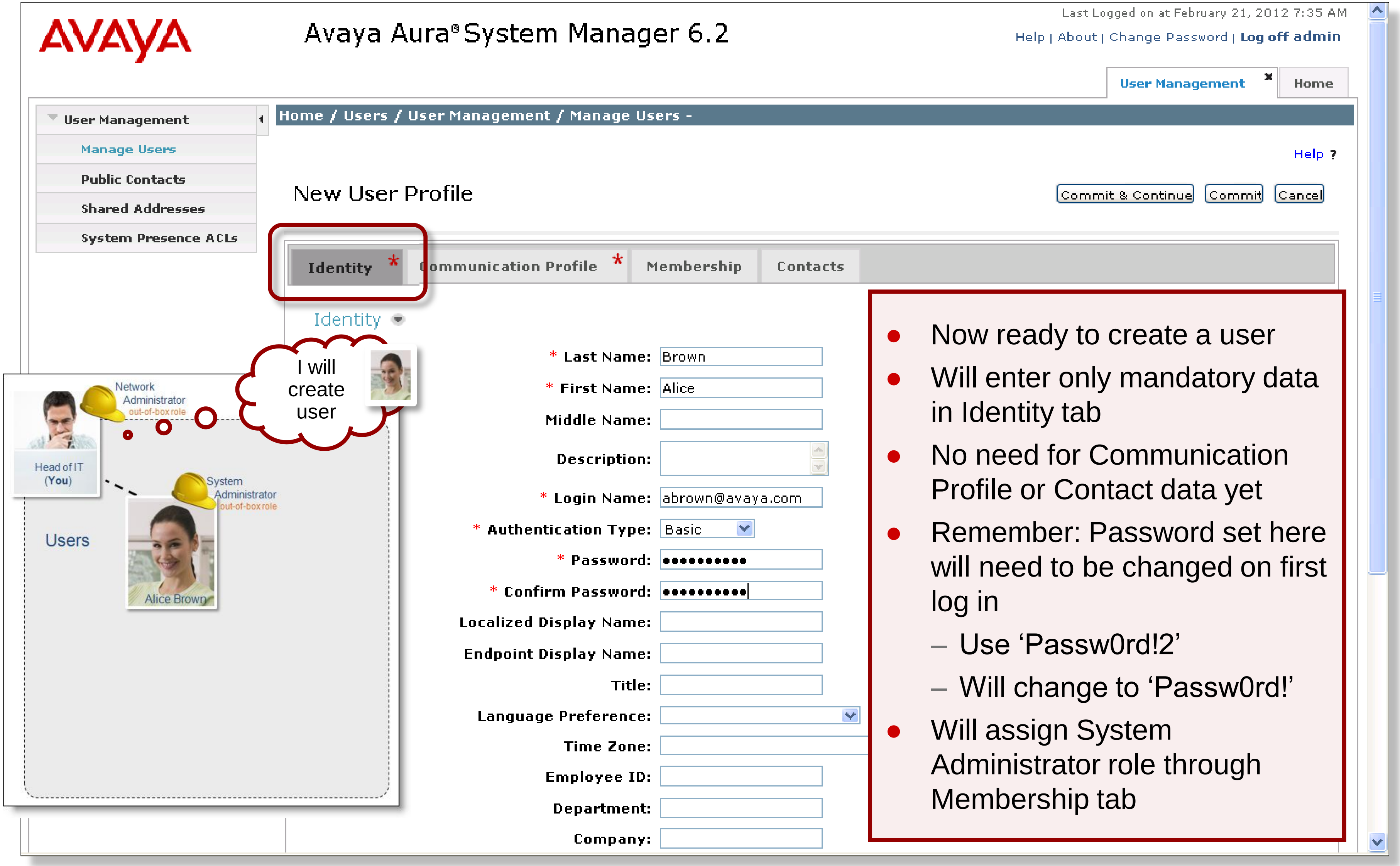
User Roles provide group-level authentication func… perform functions that are authorized for that role…

		Role Name	Users	Elements
		…or	0	All element… ReplicaGrou… All element… All element… All element… spmadmin
2	□	Avaya Services Administrator	0	
3	□	Avaya Services Maintenance and Support	0	All element… All element… All elements of type: operation
				…Manager All elements of type: IPSec Manager

We can create custom roles that provide permissions to specific resources, operations and groups.

23	□	SmAppSeqAdmin	1	All elements of type: operation	Has permissions to adminstier Session Managersequenced applications
25	□	TeamManager-ChipsTeam	1	All elements of type: users under group ChipDunnsTeam	Role to manager Chip's team of users

Practical: Creating a User



Last Logged on at February 21, 2012 7:35 AM

Avaya Aura® System Manager 6.2

New User Profile

Identity

* Last Name:	Brown
* First Name:	Alice
Middle Name:	
Description:	
* Login Name:	abrown@avaya.com
* Authentication Type:	Basic
* Password:	●●●●●●●●●●●
* Confirm Password:	●●●●●●●●●●●
Localized Display Name:	
Endpoint Display Name:	
Title:	
Language Preference:	
Time Zone:	
Employee ID:	
Department:	
Company:	

- Now ready to create a user
- Will enter only mandatory data in Identity tab
- No need for Communication Profile or Contact data yet
- Remember: Password set here will need to be changed on first log in
  - Use ‘Passw0rd!2’
  - Will change to ‘Passw0rd!’
- Will assign System Administrator role through Membership tab

Exercise: Create a System Administrator User

Objective & Outcome
The objective of this exercise is to learn to create a basic user and assign her the System Administrator role. By the time you are done, both students should have created a new System Administrator user, and should be able to log in as that user and see a Home page with all menu items (operations) available.

1. **Create new user**
   - Navigate to: Home > User Management > Manage Users. Click button ***'New'***
   - Identity tab: Enter mandatory data

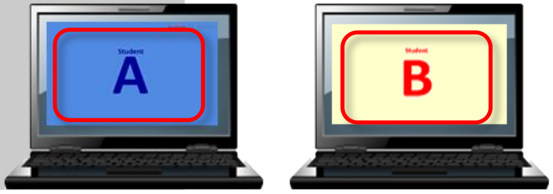
Student A - Last Name: **Brown1**
Student A - First Name: **Alice**
Student A - Login: abrown1@avaya.com
Student A - Password: **Passw0rd!2**

Student B - Last Name: **Brown2**
Student B - First Name: **Alice**
Student B - Login: abrown2@avaya.com
Student B- Password: **Passw0rd!2**

2. **Assign System Administrator Role to new user**
   - Navigate to Membership tab. Click '***Assign Roles***'
   - From Assign Roles screen: scroll down and select role '***System Administrator***'
   - Click '***Commit***'

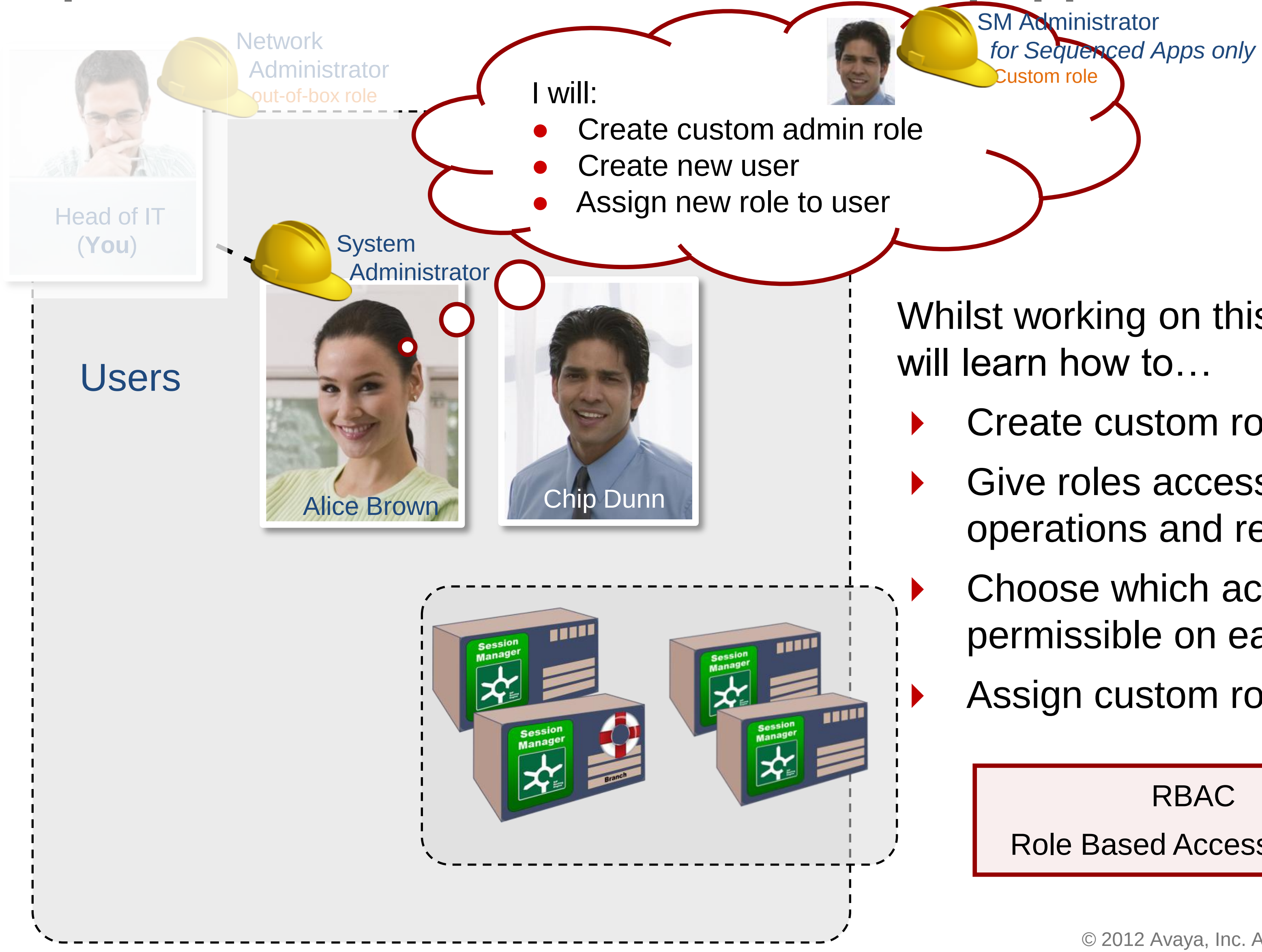
3. **Log in as new System Administrator**
   - Log off as 'admin'
   - before logging on as new System Administrator, first change the password from **Passw0rd!2** **to** **Passw0rd!** See previous exercise for tips
   - Log in with new credentials. You should see a full Home page

Individual Exercise – both students



Student A
Student B

Topic 2: Create Custom Roles – SM Seq Apps Admin



I will:

- Create custom admin role
- Create new user
- Assign new role to user

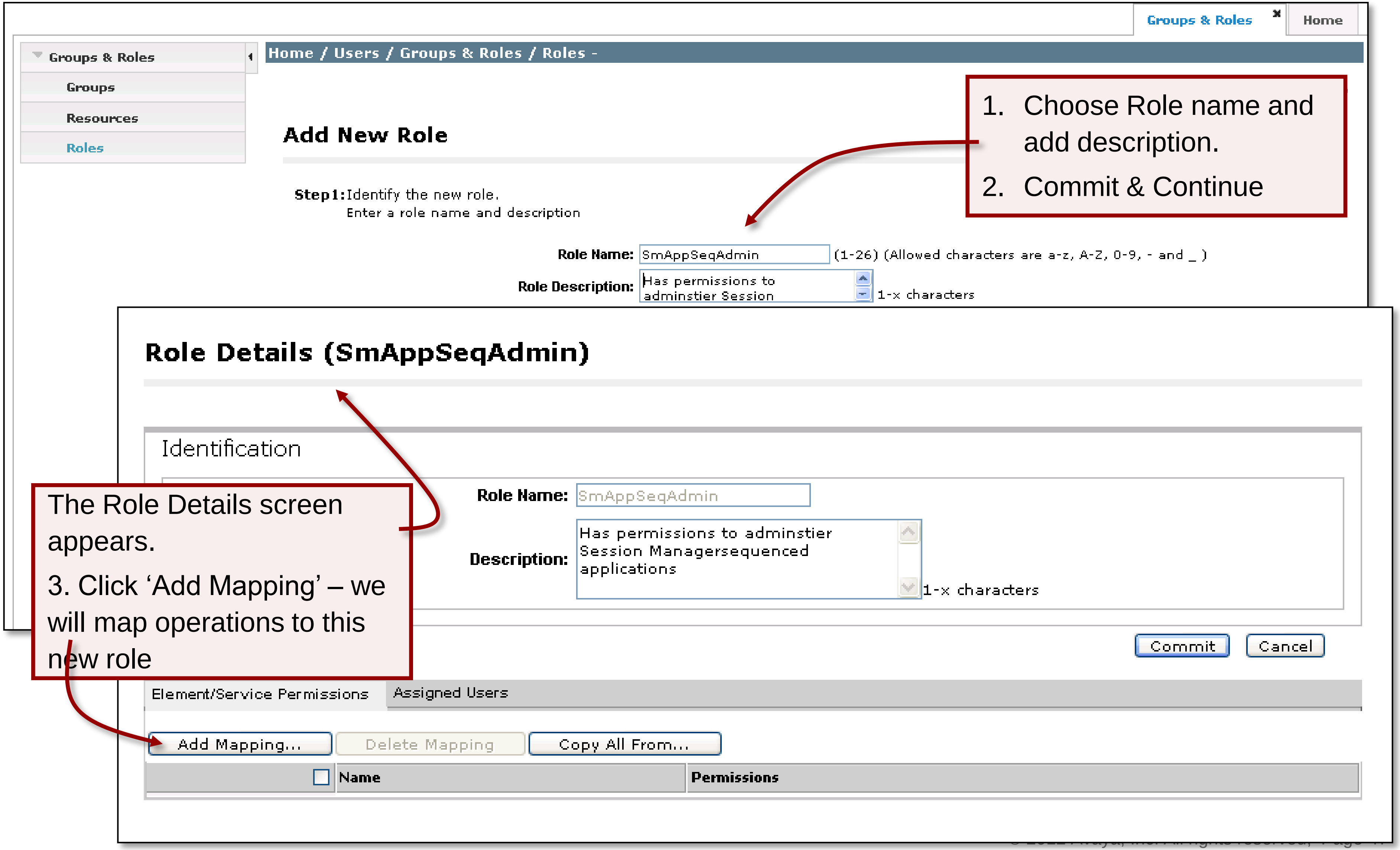
Whilst working on this topic we will learn how to…

- Create custom roles
- Give roles access to operations and resources
- Choose which actions are permissible on each resource
- Assign custom roles to a user

RBAC

Role Based Access Control

Creating a Custom Role



Add New Role

Step1: Identify the new role.
Enter a role name and description

Role Name: SmAppSeqAdmin (1-26) (Allowed characters are a-z, A-Z, 0-9, - and _)

Role Description: Has permissions to adminstier Session 1-x characters

1. Choose Role name and add description.
2. Commit & Continue

Role Details (SmAppSeqAdmin)

Identification

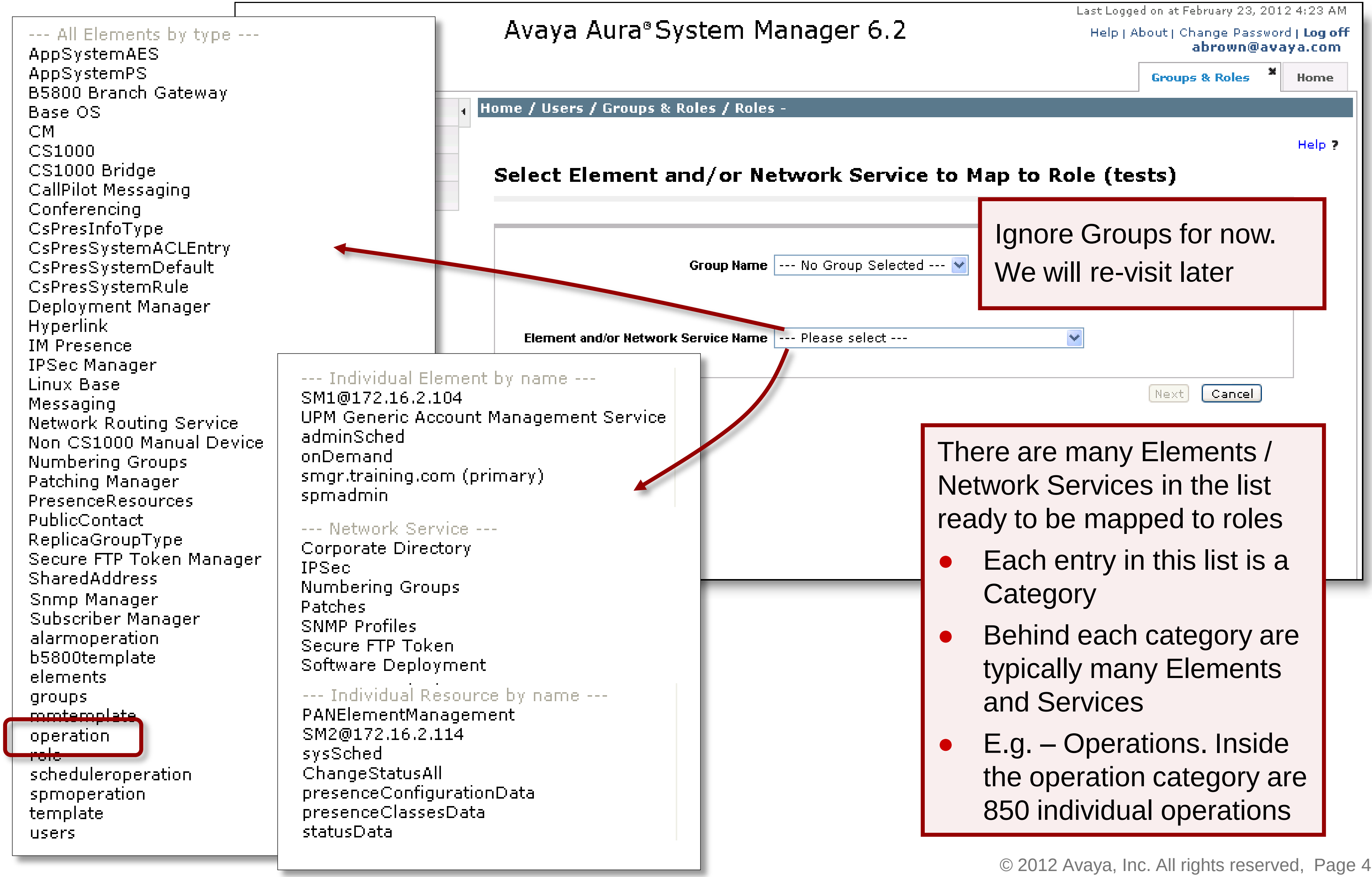
Role Name: SmAppSeqAdmin

Description: Has permissions to adminstier Session Managersequenced applications 1-x characters

The Role Details screen appears.

3. Click 'Add Mapping' – we will map operations to this new role

Elements and Network Services



Last Logged on at February 23, 2012 4:23 AM

Avaya Aura® System Manager 6.2

Help | About | Change Password | Log off
abrown@avaya.com

Home / Users / Groups & Roles / Roles -

Select Element and/or Network Service to Map to Role (tests)

Group Name: --- No Group Selected ---

Element and/or Network Service Name: --- Please select ---

--- All Elements by type ---
AppSystemAES
AppSystemPS
B5800 Branch Gateway
Base OS
CM
CS1000
CS1000 Bridge
CallPilot Messaging
Conferencing
CsPresInfoType
CsPresSystemACLEntry
CsPresSystemDefault
CsPresSystemRule
Deployment Manager
Hyperlink
IM Presence
IPSec Manager
Linux Base
Messaging
Network Routing Service
Non CS1000 Manual Device
Numbering Groups
Patching Manager
PresenceResources
PublicContact
ReplicaGroupType
Secure FTP Token Manager
SharedAddress
Snmp Manager
Subscriber Manager
alarmoperation
b5800template
elements
groups
mmtemplate
operation
role
scheduleroperation
spmoperation
template
users

--- Individual Element by name ---
SM1@172.16.2.104
UPM Generic Account Management Service
adminSched
onDemand
smgr.training.com (primary)
spmadmin

--- Network Service ---
Corporate Directory
IPSec
Numbering Groups
Patches
SNMP Profiles
Secure FTP Token
Software Deployment

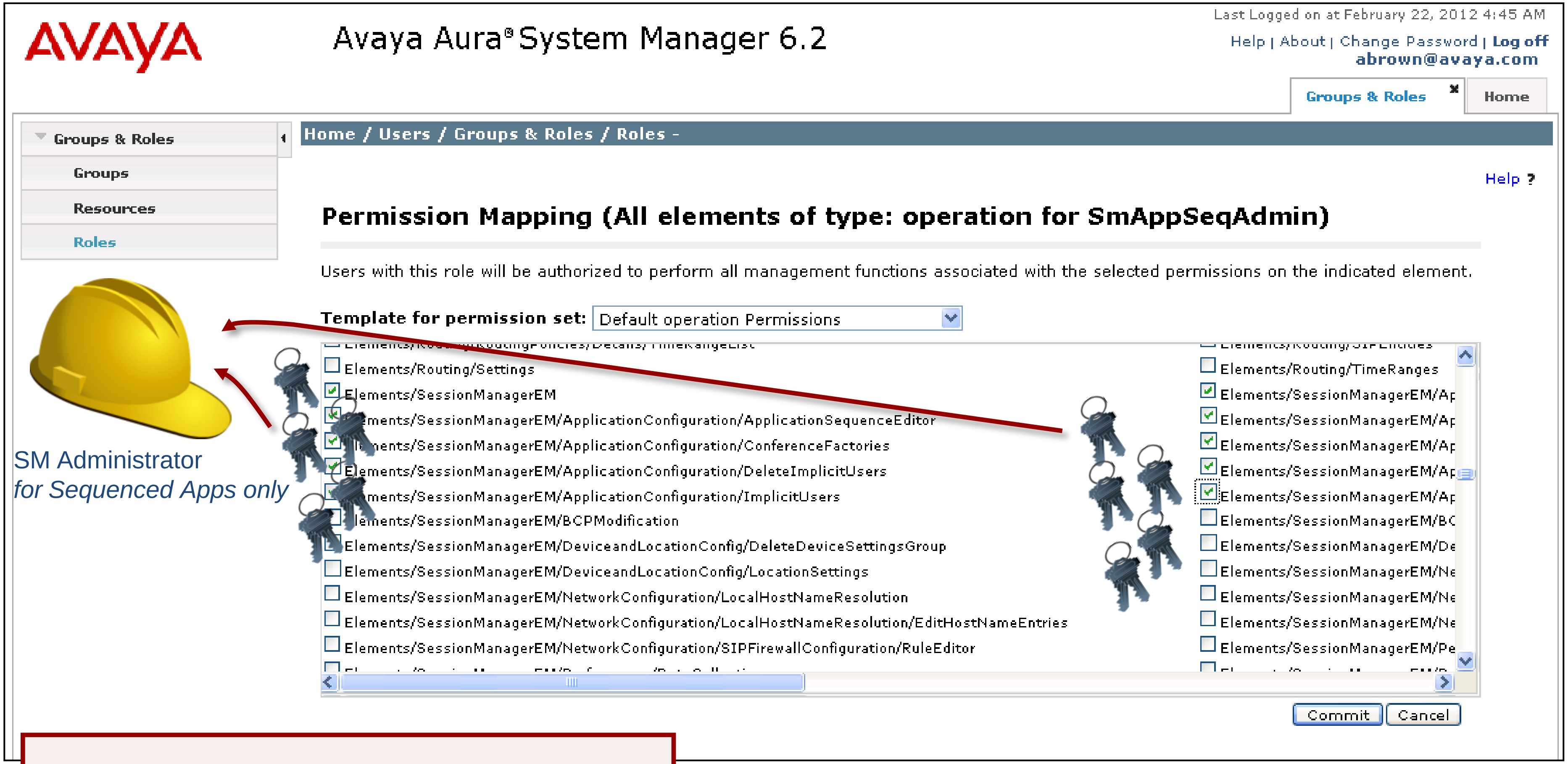
--- Individual Resource by name ---
PANElementManagement
SM2@172.16.2.114
sysSched
ChangeStatusAll
presenceConfigurationData
presenceClassesData
statusData

Ignore Groups for now.
We will re-visit later

There are many Elements / Network Services in the list ready to be mapped to roles

- Each entry in this list is a Category
- Behind each category are typically many Elements and Services
- E.g. – Operations. Inside the operation category are 850 individual operations

Adding Individual Operations to a New Role



AVAYA
Avaya Aura® System Manager 6.2
Last Logged on at February 22, 2012 4:45 AM
Help | About | Change Password | Log off
abrown@avaya.com
Groups & Roles
Home
Groups & Roles
Groups
Resources
Roles
Home / Users / Groups & Roles / Roles -
Help ?

Permission Mapping (All elements of type: operation for SmAppSeqAdmin)

Users with this role will be authorized to perform all management functions associated with the selected permissions on the indicated element.

Template for permission set: Default operation Permissions

- Elements/Routing/RoutingPolicies/Details/TimeRangeList
- □ Elements/Routing/Settings
- ☑ Elements/SessionManagerEM
- ☑ Elements/SessionManagerEM/ApplicationConfiguration/ApplicationSequenceEditor
- ☑ Elements/SessionManagerEM/ApplicationConfiguration/ConferenceFactories
- ☑ Elements/SessionManagerEM/ApplicationConfiguration/DeleteImplicitUsers
- ☑ Elements/SessionManagerEM/ApplicationConfiguration/ImplicitUsers
- □ Elements/SessionManagerEM/BCPModification
- □ Elements/SessionManagerEM/DeviceandLocationConfig/DeleteDeviceSettingsGroup
- □ Elements/SessionManagerEM/DeviceandLocationConfig/LocationSettings
- □ Elements/SessionManagerEM/NetworkConfiguration/LocalHostNameResolution
- □ Elements/SessionManagerEM/NetworkConfiguration/LocalHostNameResolution/EditHostNameEntries
- □ Elements/SessionManagerEM/NetworkConfiguration/SIPFirewallConfiguration/RuleEditor

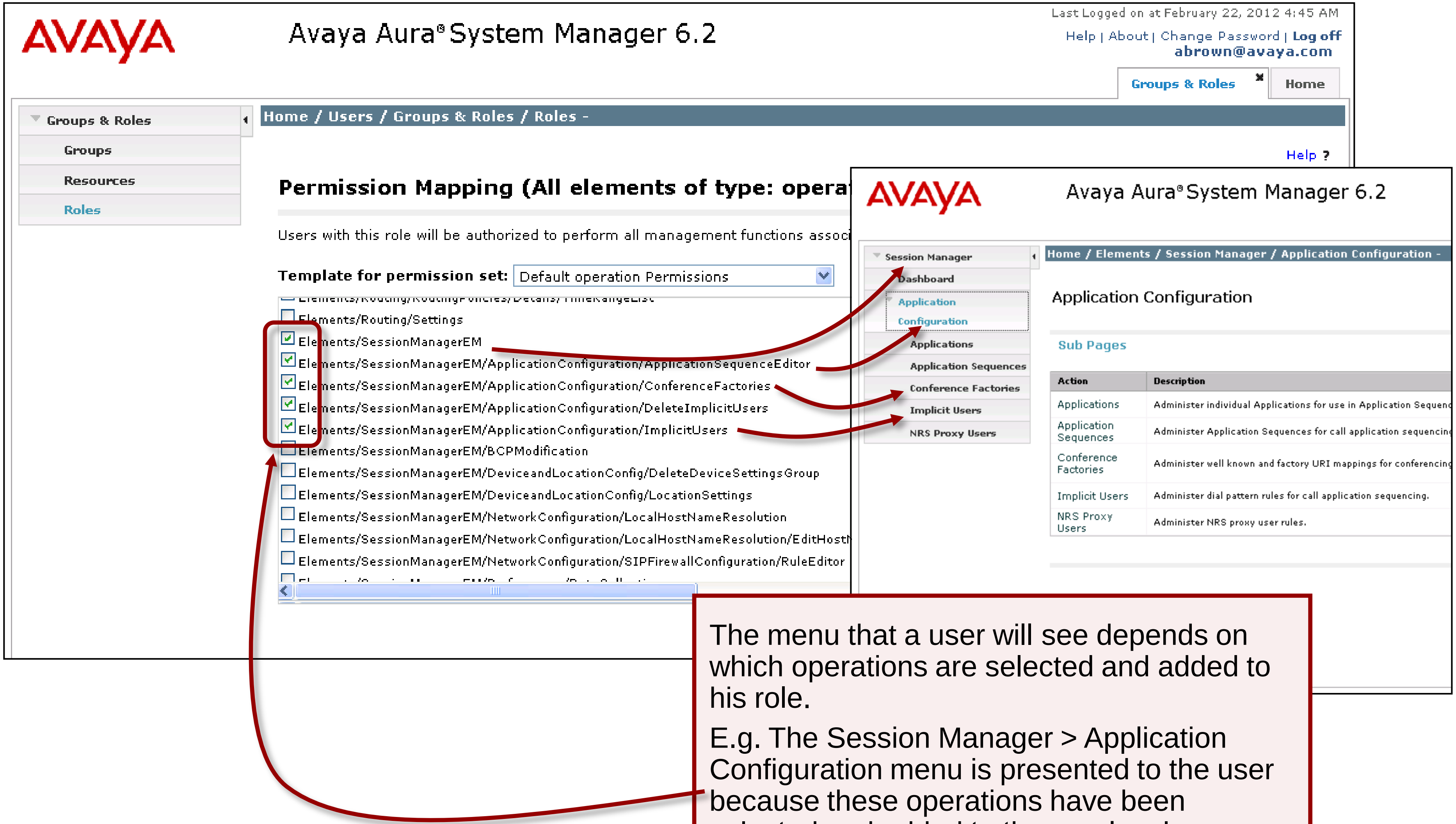
- Elements/Routing/SIPEntities
- □ Elements/Routing/TimeRanges
- ☑ Elements/SessionManagerEM/Ap
- ☑ Elements/SessionManagerEM/Ap
- ☑ Elements/SessionManagerEM/Ap
- ☑ Elements/SessionManagerEM/Ap
- ☑ Elements/SessionManagerEM/Ap
- □ Elements/SessionManagerEM/BC
- □ Elements/SessionManagerEM/De
- □ Elements/SessionManagerEM/Ne
- □ Elements/SessionManagerEM/Ne
- □ Elements/SessionManagerEM/Ne
- □ Elements/SessionManagerEM/Pe

SM Administrator
for Sequenced Apps only

Once selected and committed, each operation will be allocated to the new role.

Selecting an operation can be thought of as unlocking it for the user.

Selected Operations Define Menu Offered to User



Avaya Aura® System Manager 6.2

Last Logged on at February 22, 2012 4:45 AM

Help | About | Change Password | Log off
abrown@avaya.com

Home / Users / Groups & Roles / Roles -

Help ?

Permission Mapping (All elements of type: operat

Users with this role will be authorized to perform all management functions associ

Template for permission set: Default operation Permissions

☐ Elements/Routing/Settings
☑ Elements/SessionManagerEM
☑ Elements/SessionManagerEM/ApplicationConfiguration/ApplicationSequenceEditor
☑ Elements/SessionManagerEM/ApplicationConfiguration/ConferenceFactories
☑ Elements/SessionManagerEM/ApplicationConfiguration/DeleteImplicitUsers
☑ Elements/SessionManagerEM/ApplicationConfiguration/ImplicitUsers
☐ Elements/SessionManagerEM/BCPModification
☐ Elements/SessionManagerEM/DeviceandLocationConfig/DeleteDeviceSettingsGroup
☐ Elements/SessionManagerEM/DeviceandLocationConfig/LocationSettings
☐ Elements/SessionManagerEM/NetworkConfiguration/LocalHostNameResolution
☐ Elements/SessionManagerEM/NetworkConfiguration/LocalHostNameResolution/EditHostN
☐ Elements/SessionManagerEM/NetworkConfiguration/SIPFirewallConfiguration/RuleEditor

Avaya Aura® System Manager 6.2

Home / Elements / Session Manager / Application Configuration -

Application Configuration

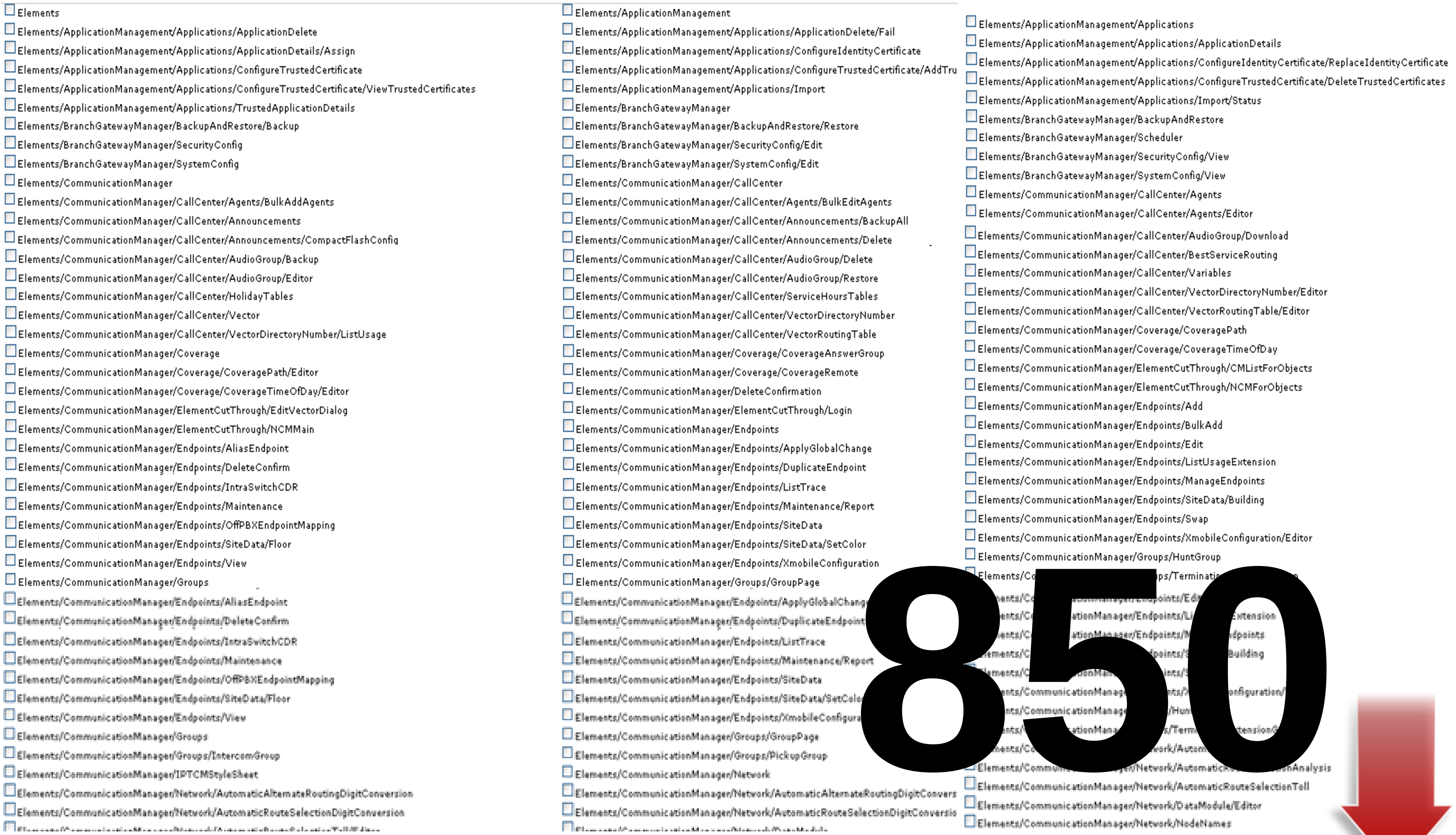
Sub Pages

Action	Description
Applications	Administer individual Applications for use in Application Sequenc
Application Sequences	Administer Application Sequences for call application sequencing
Conference Factories	Administer well known and factory URI mappings for conferencing
Implicit Users	Administer dial pattern rules for call application sequencing.
NRS Proxy Users	Administer NRS proxy user rules.

The menu that a user will see depends on which operations are selected and added to his role.

E.g. The Session Manager > Application Configuration menu is presented to the user because these operations have been selected and added to the user's role.

Operations Category – 850 Elements to Choose From!



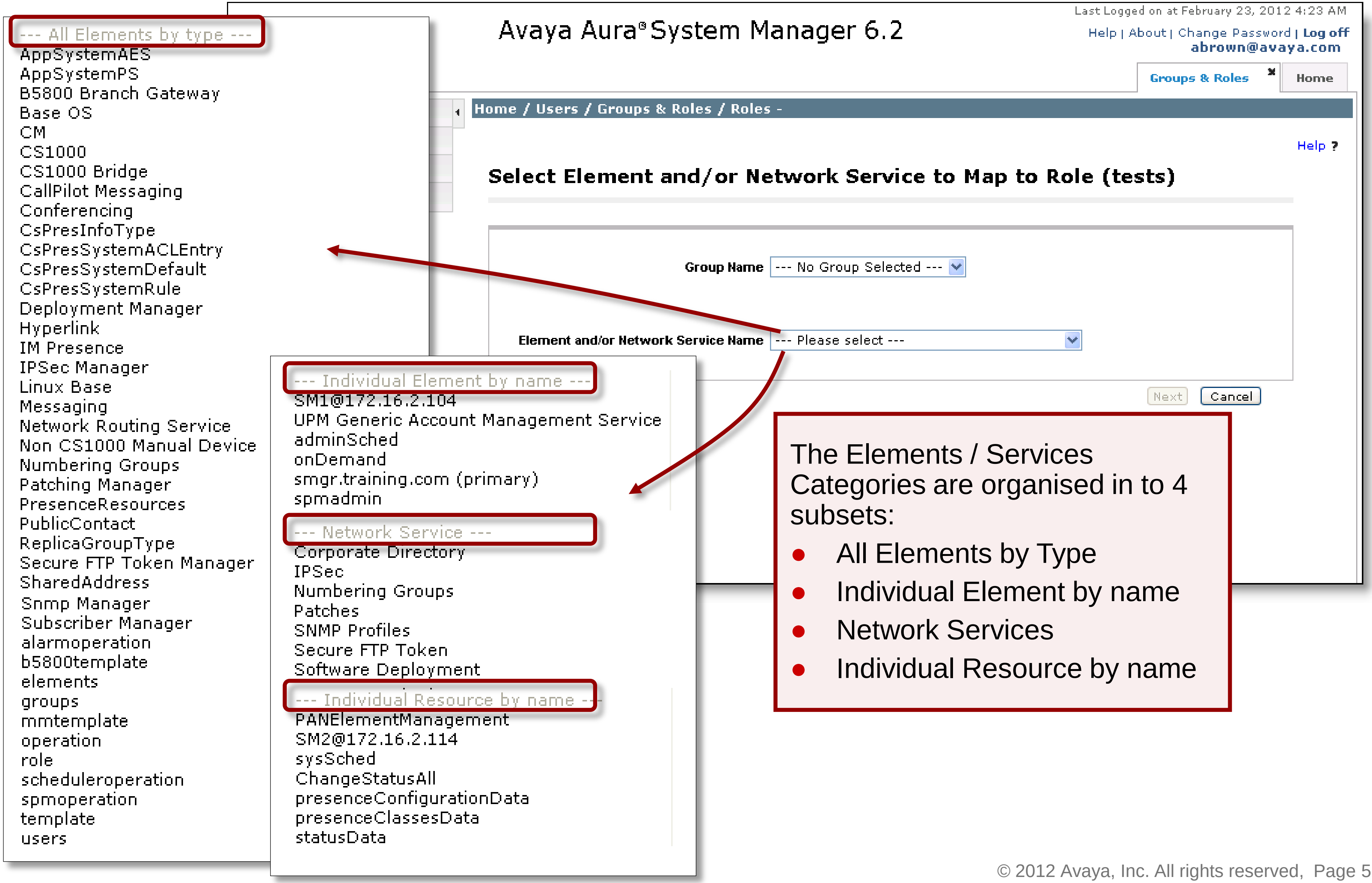
☐ Elements
☐ Elements/ApplicationManagement/Applications/ApplicationDelete
☐ Elements/ApplicationManagement/Applications/ApplicationDetails/Assign
☐ Elements/ApplicationManagement/Applications/ConfigureTrustedCertificate
☐ Elements/ApplicationManagement/Applications/ConfigureTrustedCertificate/ViewTrustedCertificates
☐ Elements/ApplicationManagement/Applications/TrustedApplicationDetails
☐ Elements/BranchGatewayManager/BackupAndRestore/Backup
☐ Elements/BranchGatewayManager/SecurityConfig
☐ Elements/BranchGatewayManager/SystemConfig
☐ Elements/CommunicationManager
☐ Elements/CommunicationManager/CallCenter/Agents/BulkAddAgents
☐ Elements/CommunicationManager/CallCenter/Announcements
☐ Elements/CommunicationManager/CallCenter/Announcements/CompactFlashConfig
☐ Elements/CommunicationManager/CallCenter/AudioGroup/Backup
☐ Elements/CommunicationManager/CallCenter/AudioGroup/Editor
☐ Elements/CommunicationManager/CallCenter/HolidayTables
☐ Elements/CommunicationManager/CallCenter/Vector
☐ Elements/CommunicationManager/CallCenter/VectorDirectoryNumber/ListUsage
☐ Elements/CommunicationManager/Coverage
☐ Elements/CommunicationManager/Coverage/CoveragePath/Editor
☐ Elements/CommunicationManager/Coverage/CoverageTimeOfDay/Editor
☐ Elements/CommunicationManager/ElementCutThrough/EditVectorDialog
☐ Elements/CommunicationManager/ElementCutThrough/NCMMain
☐ Elements/CommunicationManager/Endpoints/AliasEndpoint
☐ Elements/CommunicationManager/Endpoints/DeleteConfirm
☐ Elements/CommunicationManager/Endpoints/IntraSwitchCDR
☐ Elements/CommunicationManager/Endpoints/Maintenance
☐ Elements/CommunicationManager/Endpoints/OffPBXEndpointMapping
☐ Elements/CommunicationManager/Endpoints/SiteData/Floor
☐ Elements/CommunicationManager/Endpoints/View
☐ Elements/CommunicationManager/Groups
☐ Elements/CommunicationManager/Endpoints/AliasEndpoint
☐ Elements/CommunicationManager/Endpoints/DeleteConfirm
☐ Elements/CommunicationManager/Endpoints/IntraSwitchCDR
☐ Elements/CommunicationManager/Endpoints/Maintenance
☐ Elements/CommunicationManager/Endpoints/OffPBXEndpointMapping
☐ Elements/CommunicationManager/Endpoints/SiteData/Floor
☐ Elements/CommunicationManager/Endpoints/View
☐ Elements/CommunicationManager/Groups
☐ Elements/CommunicationManager/Groups/IntercomGroup
☐ Elements/CommunicationManager/IPTCMStyleSheet
☐ Elements/CommunicationManager/Network/AutomaticAlternateRoutingDigitConversion
☐ Elements/CommunicationManager/Network/AutomaticRouteSelectionDigitConversion
☐ Elements/CommunicationManager/Network/AutomaticRouteSelectionToll/Editor

☐ Elements/ApplicationManagement
☐ Elements/ApplicationManagement/Applications/ApplicationDelete/Fail
☐ Elements/ApplicationManagement/Applications/ConfigureIdentityCertificate
☐ Elements/ApplicationManagement/Applications/ConfigureTrustedCertificate/AddTru
☐ Elements/ApplicationManagement/Applications/Import
☐ Elements/BranchGatewayManager
☐ Elements/BranchGatewayManager/BackupAndRestore/Restore
☐ Elements/BranchGatewayManager/SecurityConfig/Edit
☐ Elements/BranchGatewayManager/SystemConfig/Edit
☐ Elements/CommunicationManager/CallCenter
☐ Elements/CommunicationManager/CallCenter/Agents/BulkEditAgents
☐ Elements/CommunicationManager/CallCenter/Announcements/BackupAll
☐ Elements/CommunicationManager/CallCenter/Announcements/Delete
☐ Elements/CommunicationManager/CallCenter/AudioGroup/Delete
☐ Elements/CommunicationManager/CallCenter/AudioGroup/Restore
☐ Elements/CommunicationManager/CallCenter/ServiceHoursTables
☐ Elements/CommunicationManager/CallCenter/VectorDirectoryNumber
☐ Elements/CommunicationManager/CallCenter/VectorRoutingTable
☐ Elements/CommunicationManager/Coverage/CoverageAnswerGroup
☐ Elements/CommunicationManager/Coverage/CoverageRemote
☐ Elements/CommunicationManager/DeleteConfirmation
☐ Elements/CommunicationManager/ElementCutThrough/Login
☐ Elements/CommunicationManager/Endpoints
☐ Elements/CommunicationManager/Endpoints/ApplyGlobalChange
☐ Elements/CommunicationManager/Endpoints/DuplicateEndpoint
☐ Elements/CommunicationManager/Endpoints/ListTrace
☐ Elements/CommunicationManager/Endpoints/Maintenance/Report
☐ Elements/CommunicationManager/Endpoints/SiteData
☐ Elements/CommunicationManager/Endpoints/SiteData/SetColor
☐ Elements/CommunicationManager/Endpoints/XmobileConfiguration
☐ Elements/CommunicationManager/Groups/GroupPage
☐ Elements/CommunicationManager/Endpoints/ApplyGlobalChang
☐ Elements/CommunicationManager/Endpoints/DuplicateEndpoint
☐ Elements/CommunicationManager/Endpoints/ListTrace
☐ Elements/CommunicationManager/Endpoints/Maintenance/Report
☐ Elements/CommunicationManager/Endpoints/SiteData
☐ Elements/CommunicationManager/Endpoints/SiteData/SetColo
☐ Elements/CommunicationManager/Endpoints/XmobileConfigura
☐ Elements/CommunicationManager/Groups/GroupPage
☐ Elements/CommunicationManager/Groups/PickupGroup
☐ Elements/CommunicationManager/Network
☐ Elements/CommunicationManager/Network/AutomaticAlternateRoutingDigitConvers
☐ Elements/CommunicationManager/Network/AutomaticRouteSelectionDigitConversio
☐ Elements/CommunicationManager/Network/DataModule

☐ Elements/ApplicationManagement/Applications
☐ Elements/ApplicationManagement/Applications/ApplicationDetails
☐ Elements/ApplicationManagement/Applications/ConfigureIdentityCertificate/ReplaceIdentityCertificate
☐ Elements/ApplicationManagement/Applications/ConfigureTrustedCertificate/DeleteTrustedCertificates
☐ Elements/ApplicationManagement/Applications/Import/Status
☐ Elements/BranchGatewayManager/BackupAndRestore
☐ Elements/BranchGatewayManager/Scheduler
☐ Elements/BranchGatewayManager/SecurityConfig/View
☐ Elements/BranchGatewayManager/SystemConfig/View
☐ Elements/CommunicationManager/CallCenter/Agents
☐ Elements/CommunicationManager/CallCenter/Agents/Editor
☐ Elements/CommunicationManager/CallCenter/AudioGroup/Download
☐ Elements/CommunicationManager/CallCenter/BestServiceRouting
☐ Elements/CommunicationManager/CallCenter/Variables
☐ Elements/CommunicationManager/CallCenter/VectorDirectoryNumber/Editor
☐ Elements/CommunicationManager/CallCenter/VectorRoutingTable/Editor
☐ Elements/CommunicationManager/Coverage/CoveragePath
☐ Elements/CommunicationManager/Coverage/CoverageTimeOfDay
☐ Elements/CommunicationManager/ElementCutThrough/CMListForObjects
☐ Elements/CommunicationManager/ElementCutThrough/NCMForObjects
☐ Elements/CommunicationManager/Endpoints/Add
☐ Elements/CommunicationManager/Endpoints/BulkAdd
☐ Elements/CommunicationManager/Endpoints/Edit
☐ Elements/CommunicationManager/Endpoints/ListUsageExtension
☐ Elements/CommunicationManager/Endpoints/ManageEndpoints
☐ Elements/CommunicationManager/Endpoints/SiteData/Building
☐ Elements/CommunicationManager/Endpoints/Swap
☐ Elements/CommunicationManager/Endpoints/XmobileConfiguration/Editor
☐ Elements/CommunicationManager/Groups/HuntGroup
☐ Elements/Co[illegible]ps/Terminati[illegible]
[illegible]ents/Co[illegible]Endpoints/Ed[illegible]
[illegible]ents/Co[illegible]ationManager/Endpoints/Li[illegible]Extension
[illegible]ents/Co[illegible]ationManager/Endpoints/M[illegible]dpoints
[illegible]lements/C[illegible]dpoints/S[illegible]Building
[illegible]lements/C[illegible]ionMan[illegible]ints/S[illegible]
[illegible]ents/CommunicationManage[illegible]nts/X[illegible]onfiguration/[illegible]
[illegible]nts/CommunicationManage[illegible]/Hun[illegible]
[illegible]nts/[illegible]ationMana[illegible]s/Term[illegible]tension[illegible]
[illegible]ments/Co[illegible]twork/Autom[illegible]
☐ Elements/Commun[illegible]ger/Network/AutomaticR[illegible]onAnalysis
☐ Elements/CommunicationManager/Network/AutomaticRouteSelectionToll
☐ Elements/CommunicationManager/Network/DataModule/Editor
☐ Elements/CommunicationManager/Network/NodeNames

850

Elements and Network Services



Last Logged on at February 23, 2012 4:23 AM

Avaya Aura® System Manager 6.2

Help | About | Change Password | Log off
abrown@avaya.com

Home / Users / Groups & Roles / Roles -

Select Element and/or Network Service to Map to Role (tests)

Group Name: --- No Group Selected ---

Element and/or Network Service Name: --- Please select ---

--- All Elements by type ---
AppSystemAES
AppSystemPS
B5800 Branch Gateway
Base OS
CM
CS1000
CS1000 Bridge
CallPilot Messaging
Conferencing
CsPresInfoType
CsPresSystemACLEntry
CsPresSystemDefault
CsPresSystemRule
Deployment Manager
Hyperlink
IM Presence
IPSec Manager
Linux Base
Messaging
Network Routing Service
Non CS1000 Manual Device
Numbering Groups
Patching Manager
PresenceResources
PublicContact
ReplicaGroupType
Secure FTP Token Manager
SharedAddress
Snmp Manager
Subscriber Manager
alarmoperation
b5800template
elements
groups
mmtemplate
operation
role
scheduleroperation
spmoperation
template
users

--- Individual Element by name ---
SM1@172.16.2.104
UPM Generic Account Management Service
adminSched
onDemand
smgr.training.com (primary)
spmadmin

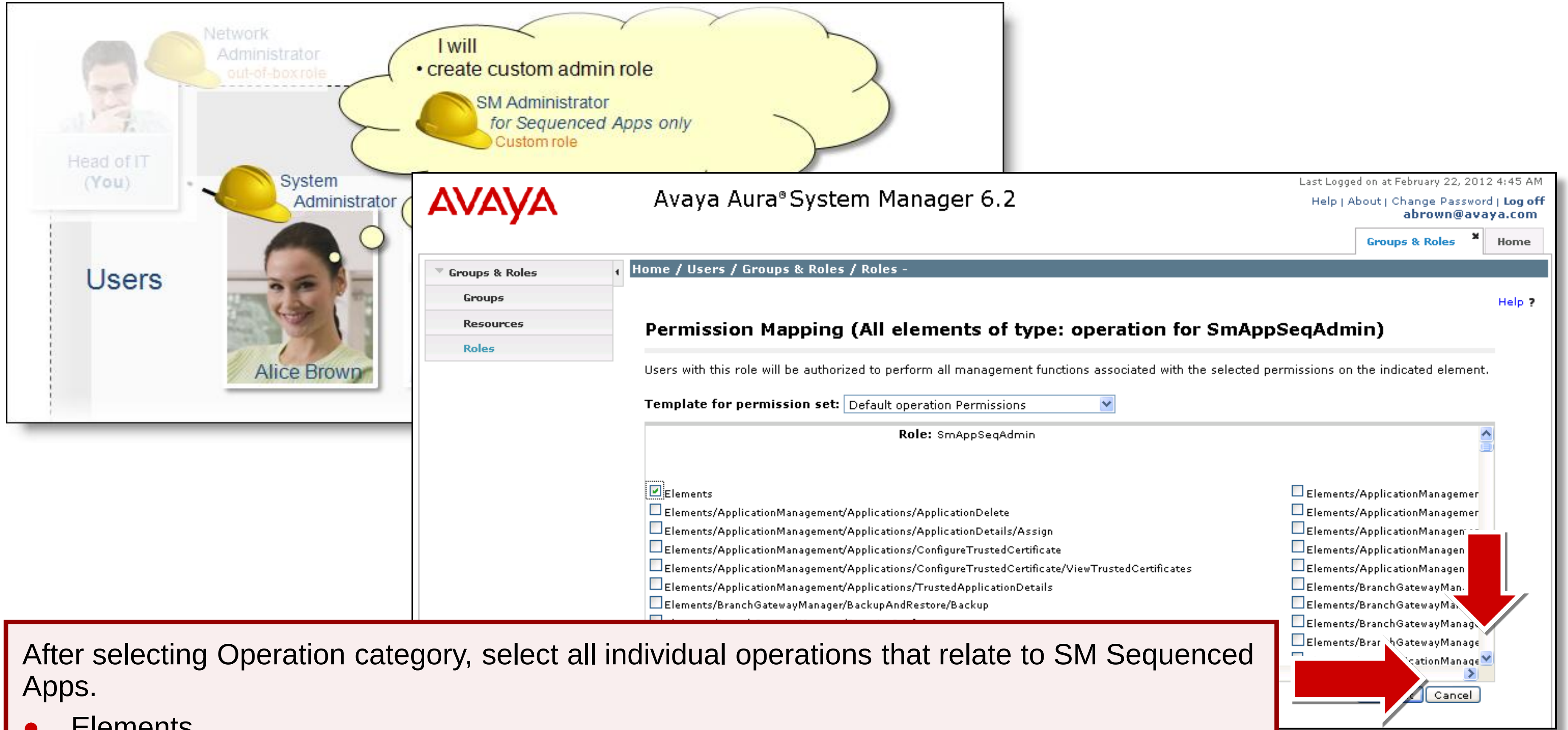
--- Network Service ---
Corporate Directory
IPSec
Numbering Groups
Patches
SNMP Profiles
Secure FTP Token
Software Deployment

--- Individual Resource by name ---
PANElementManagement
SM2@172.16.2.114
sysSched
ChangeStatusAll
presenceConfigurationData
presenceClassesData
statusData

The Elements / Services Categories are organised in to 4 subsets:

- All Elements by Type
- Individual Element by name
- Network Services
- Individual Resource by name

Practical: Creating a Custom Role



AVAYA Avaya Aura® System Manager 6.2

Last Logged on at February 22, 2012 4:45 AM
Help | About | Change Password | Log off
abrown@avaya.com

Groups & Roles | Home

Groups & Roles
- Groups
- Resources
- Roles

Home / Users / Groups & Roles / Roles -

Help ?

Permission Mapping (All elements of type: operation for SmAppSeqAdmin)

Users with this role will be authorized to perform all management functions associated with the selected permissions on the indicated element.

Template for permission set: Default operation Permissions

Role: SmAppSeqAdmin

☑ Elements
□ Elements/ApplicationManagement/Applications/ApplicationDelete
□ Elements/ApplicationManagement/Applications/ApplicationDetails/Assign
□ Elements/ApplicationManagement/Applications/ConfigureTrustedCertificate
□ Elements/ApplicationManagement/Applications/ConfigureTrustedCertificate/ViewTrustedCertificates
□ Elements/ApplicationManagement/Applications/TrustedApplicationDetails
□ Elements/BranchGatewayManager/BackupAndRestore/Backup

□ Elements/ApplicationManagemer
□ Elements/ApplicationManagemer
□ Elements/ApplicationManagem
□ Elements/ApplicationManagen
□ Elements/ApplicationManagen
□ Elements/BranchGatewayMan.
□ Elements/BranchGatewayMa
□ Elements/BranchGatewayManag
□ Elements/Brar hGatewayManage
cationManage

Cancel

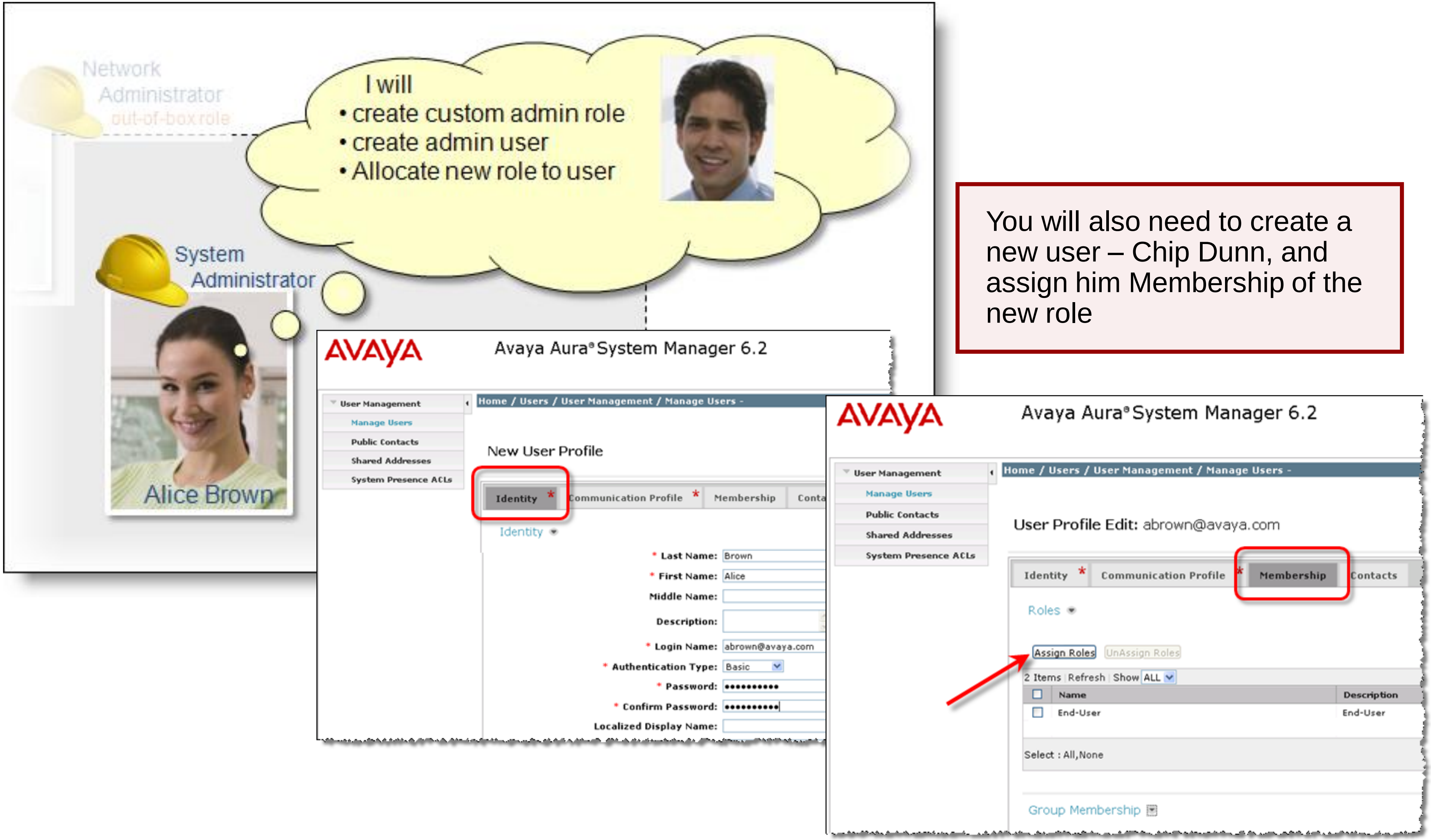
After selecting Operation category, select all individual operations that relate to SM Sequenced Apps.

- Elements
- Elements/SessionManagerEM
- All operations beginning with Elements/SessionManagerEM/ApplicationConfiguration (there are 14)
- All operations beginning with Elements/SessionManagerEM/SMDashboard (there are 2)

Students will need to scroll across (3 columns) and scroll down to find them all.

Practical: Creating a User and Assigning a Role

You will also need to create a new user – Chip Dunn, and assign him Membership of the new role



AVAYA Avaya Aura® System Manager 6.2

- User Management
  - Manage Users
  - Public Contacts
  - Shared Addresses
  - System Presence ACLs

Home / Users / User Management / Manage Users -

New User Profile

Identity * | Communication Profile * | Membership | Conta

Identity

* Last Name: Brown
* First Name: Alice
Middle Name:
Description:
* Login Name: abrown@avaya.com
* Authentication Type: Basic
* Password: ••••••••••
* Confirm Password: ••••••••••
Localized Display Name:

AVAYA Avaya Aura® System Manager 6.2

- User Management
  - Manage Users
  - Public Contacts
  - Shared Addresses
  - System Presence ACLs

Home / Users / User Management / Manage Users -

User Profile Edit: abrown@avaya.com

Identity * | Communication Profile * | Membership | Contacts

Roles

Assign Roles | UnAssign Roles

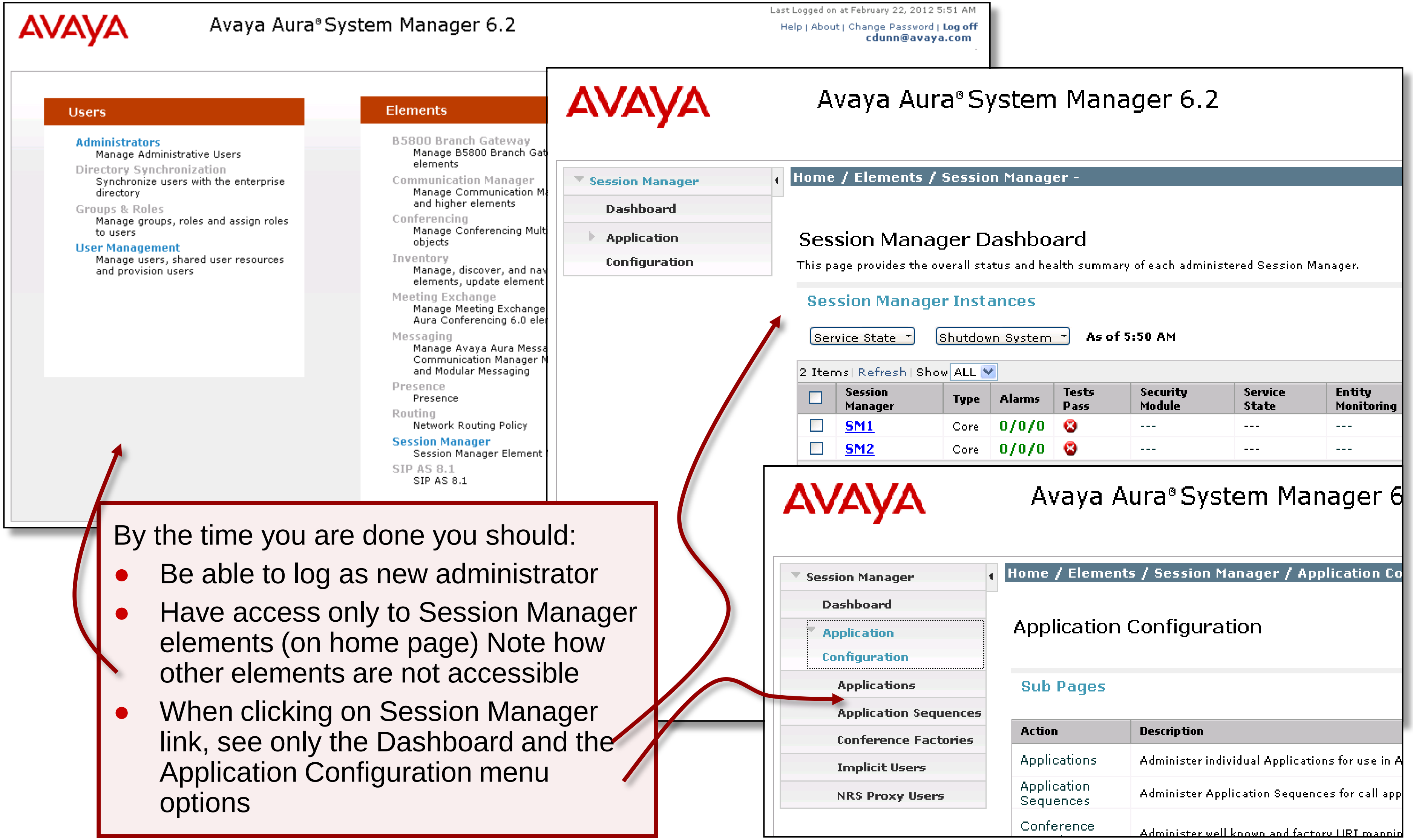
2 Items | Refresh | Show ALL

□	Name	Description
□	End-User	End-User

Select : All, None

Group Membership

Practical: Creating a Custom Role – Expected Outcomes



AVAYA Avaya Aura® System Manager 6.2

Last Logged on at February 22, 2012 5:51 AM
Help | About | Change Password | Log off
cdunn@avaya.com

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

B5800 Branch Gateway
Manage B5800 Branch Gat
elements

Communication Manager
Manage Communication M
and higher elements

Conferencing
Manage Conferencing Mult
objects

Inventory
Manage, discover, and nav
elements, update element

Meeting Exchange
Manage Meeting Exchange
Aura Conferencing 6.0 ele

Messaging
Manage Avaya Aura Messa
Communication Manager M
and Modular Messaging

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element

SIP AS 8.1
SIP AS 8.1

AVAYA Avaya Aura® System Manager 6.2

Home / Elements / Session Manager -

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State ▾ Shutdown System ▾ As of 5:50 AM

2 Items | Refresh | Show ALL ▾

□	Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring
□	SM1	Core	0/0/0	☒	---	---	---
□	SM2	Core	0/0/0	☒	---	---	---

AVAYA Avaya Aura® System Manager 6

Home / Elements / Session Manager / Application Co

Application Configuration

Sub Pages

Action	Description
Applications	Administer individual Applications for use in A
Application Sequences	Administer Application Sequences for call app
Conference	Administer well known and factory URI mappin

By the time you are done you should:

- Be able to log as new administrator
- Have access only to Session Manager elements (on home page) Note how other elements are not accessible
- When clicking on Session Manager link, see only the Dashboard and the Application Configuration menu options

Exercise: Create & Assign a Custom SM SeqAppAdmin Role

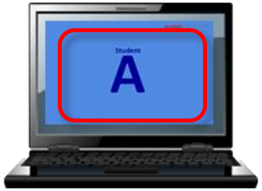
Objective & Outcome
The objective is to learn to use RBAC. You will create a custom role that will permit a user to administer Session Manager's Sequenced Applications. When done, you will log in as the new user and have access only to the Session Manager Sequenced Applications operations.

1. Create custom role
   - Navigate to: Home > Groups & Roles > Roles. Click button 'Add'.
   - Enter Role Name '**SmAppSeqAdminA'** or '**SmAppSeqAdminB'.** Click '***Commit and Continue'***
   - Click button '***Add Mapping***'. (Leave Group Name unselected).
   - Select '**operation**' from Element list. Click '***Next***'.
   - From Permission Mapping screen, select all of the following operations
     * ***Elements***
     **** Elements/SessionManagerEM***
     * the 14 ops that begin with ***Elements/SessionManagerEM/ApplicationConfiguration***
     * The 2 ops that begin with ***Elements/SessionManagerEM/SMDashboard***
   - **Commit**
   - Scroll down and check the new Role '**SmAppSeqAdmin'** is showing in the list.

2. Create new user
   - Navigate to: Home > User Management > Manage Users. Click button '**New**'
   - Identity tab: Enter mandatory data – **Chip, Dunn1/2**, cdunn1/2@avaya.com, **Passw0rd!2**
   - Assign the role **SmAppSeqAdmina/b**
   - **Commit**

3. Login as new user and check you have permissions for Session Manager Applications
   - Log out as abrown. Change **cdunn1/2@avaya.com**'s password from **Passw0rd!2** to **Passw0rd!** And login as Chip Dunn.
   - Check that Session Manager is the only Element available on the Home Page
   - Click 'Session Manager' link and test that you only have access to Session Manager Apps

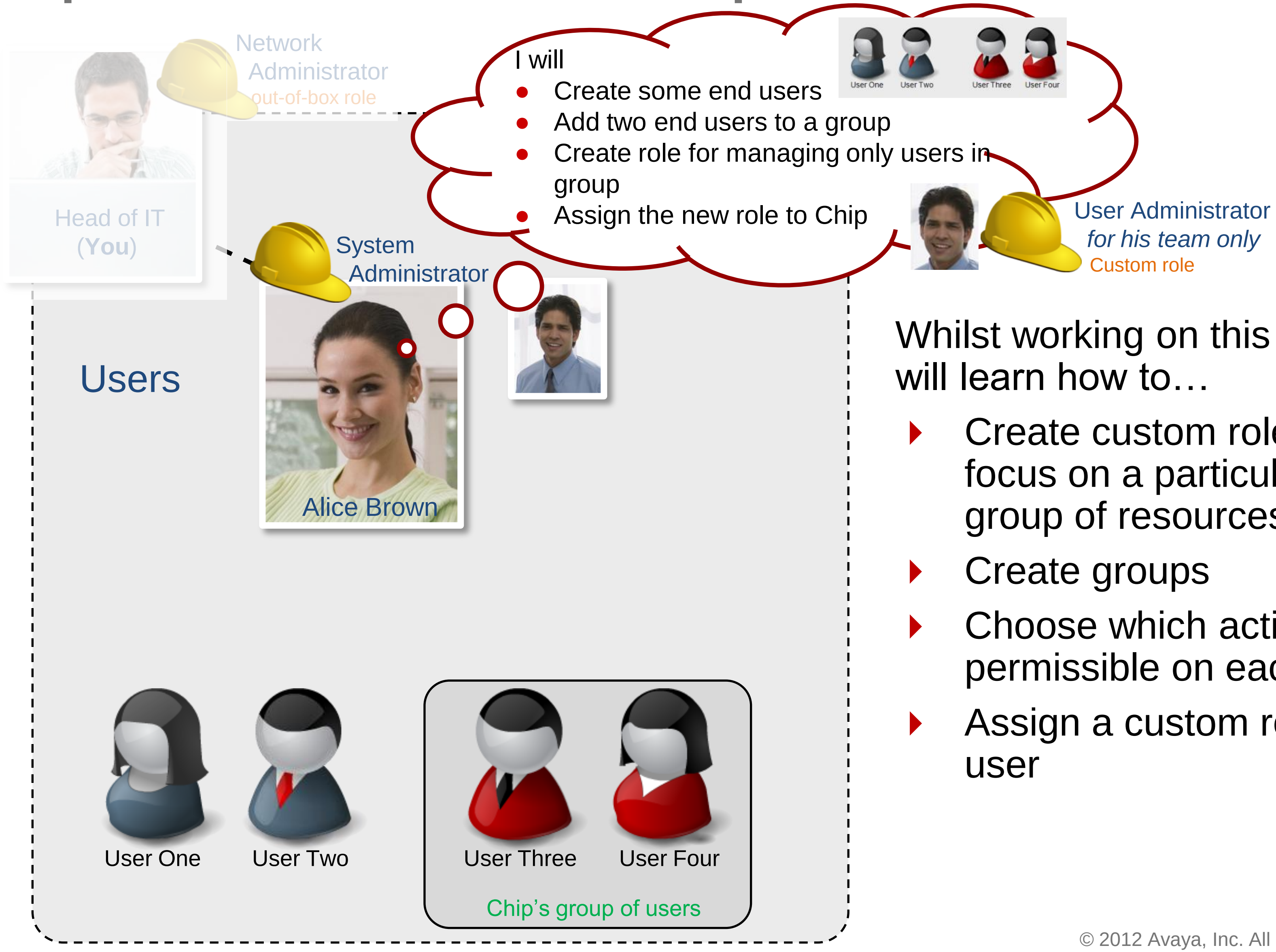
Individual Exercise – both students can work simultaneously



Student A

Student B

Topic 3: Create Custom ‘Group Based’ Role – User Admin

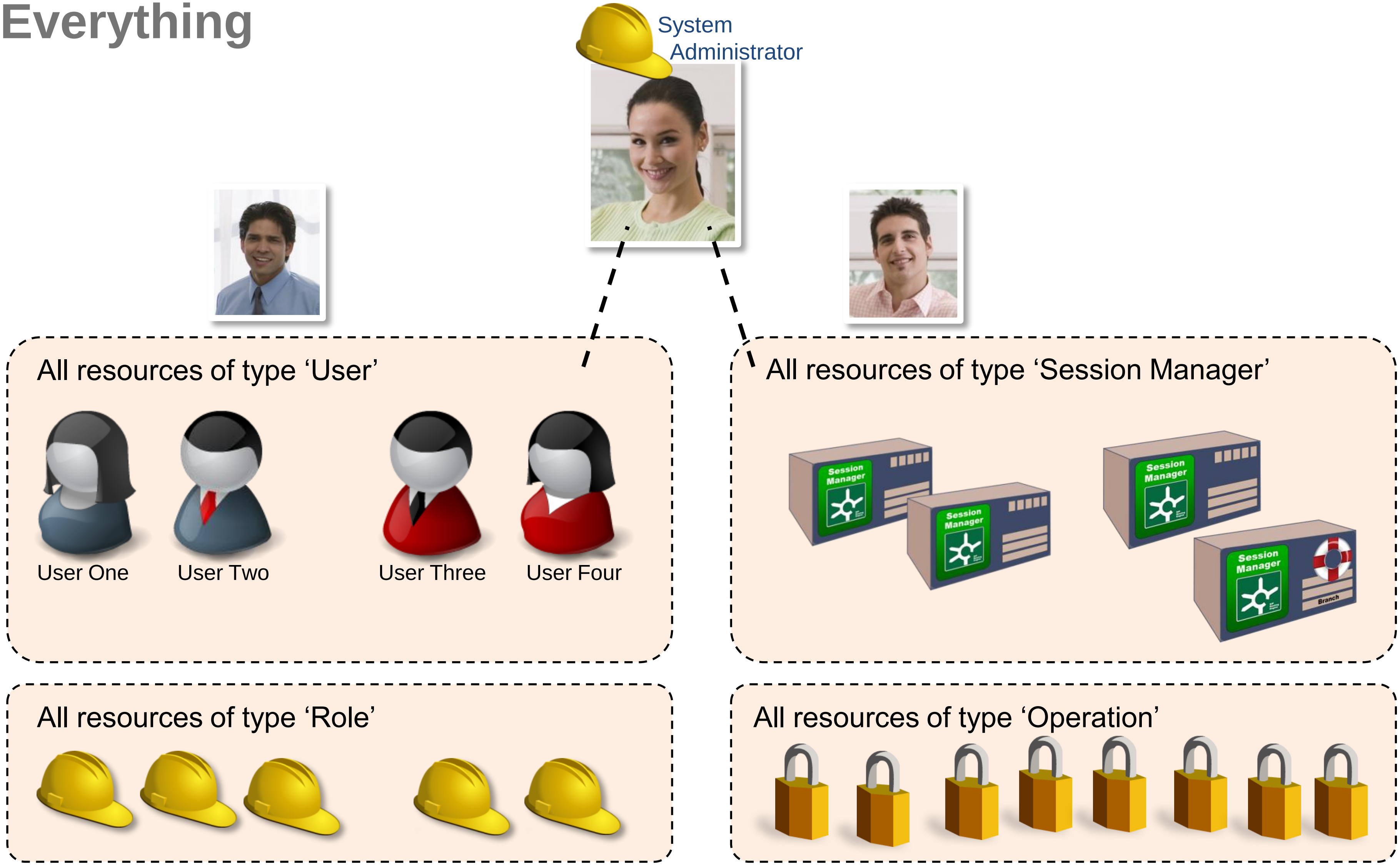


I will
- Create some end users
- Add two end users to a group
- Create role for managing only users in group
- Assign the new role to Chip

Whilst working on this topic we will learn how to…

- Create custom roles that focus on a particular sub-group of resources
- Create groups
- Choose which actions are permissible on each group
- Assign a custom role to a user

SMGR Resources – System Admin has Access to Everything



System Administrator

All resources of type ‘User’

User One

User Two

User Three

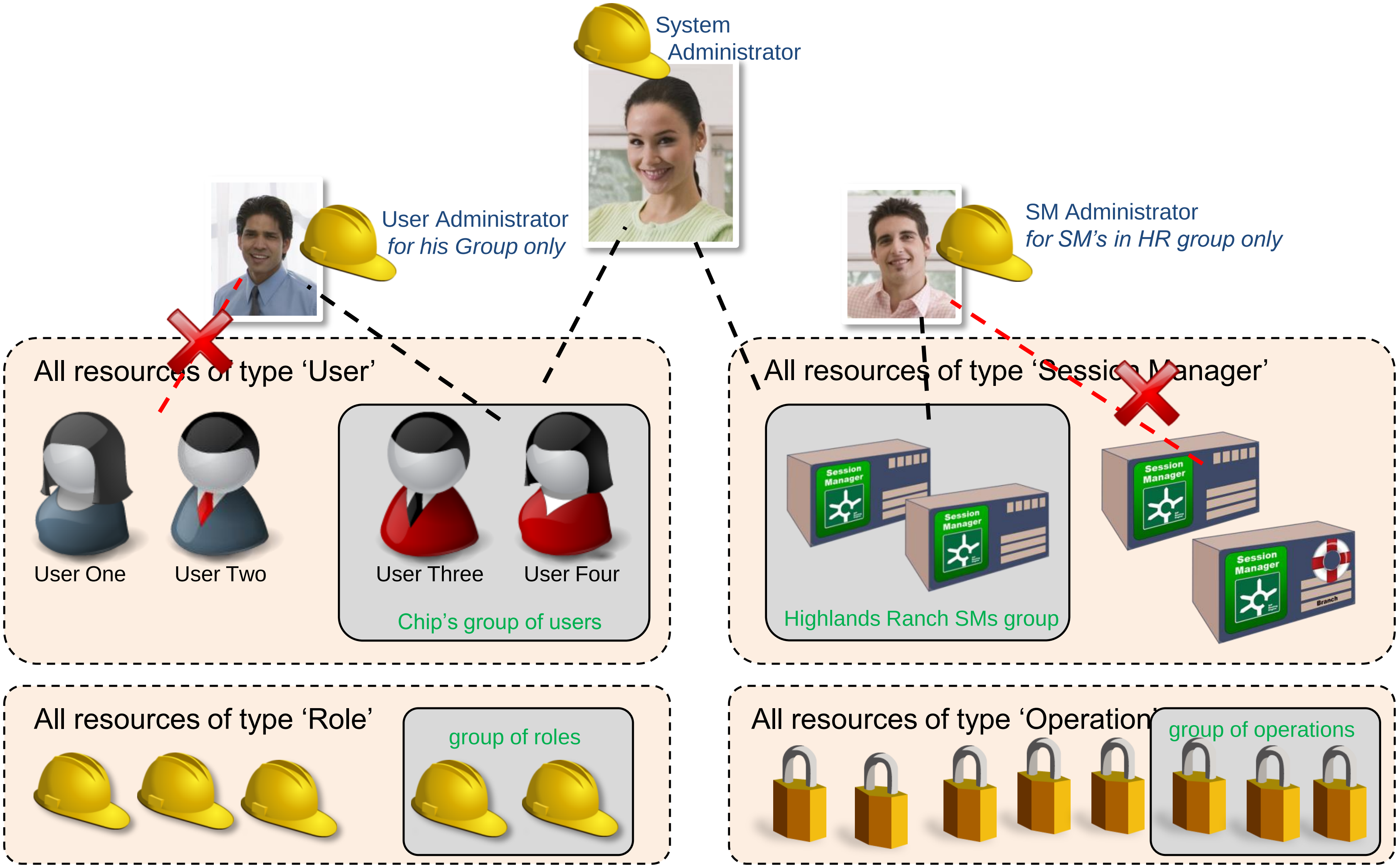
User Four

All resources of type ‘Session Manager’

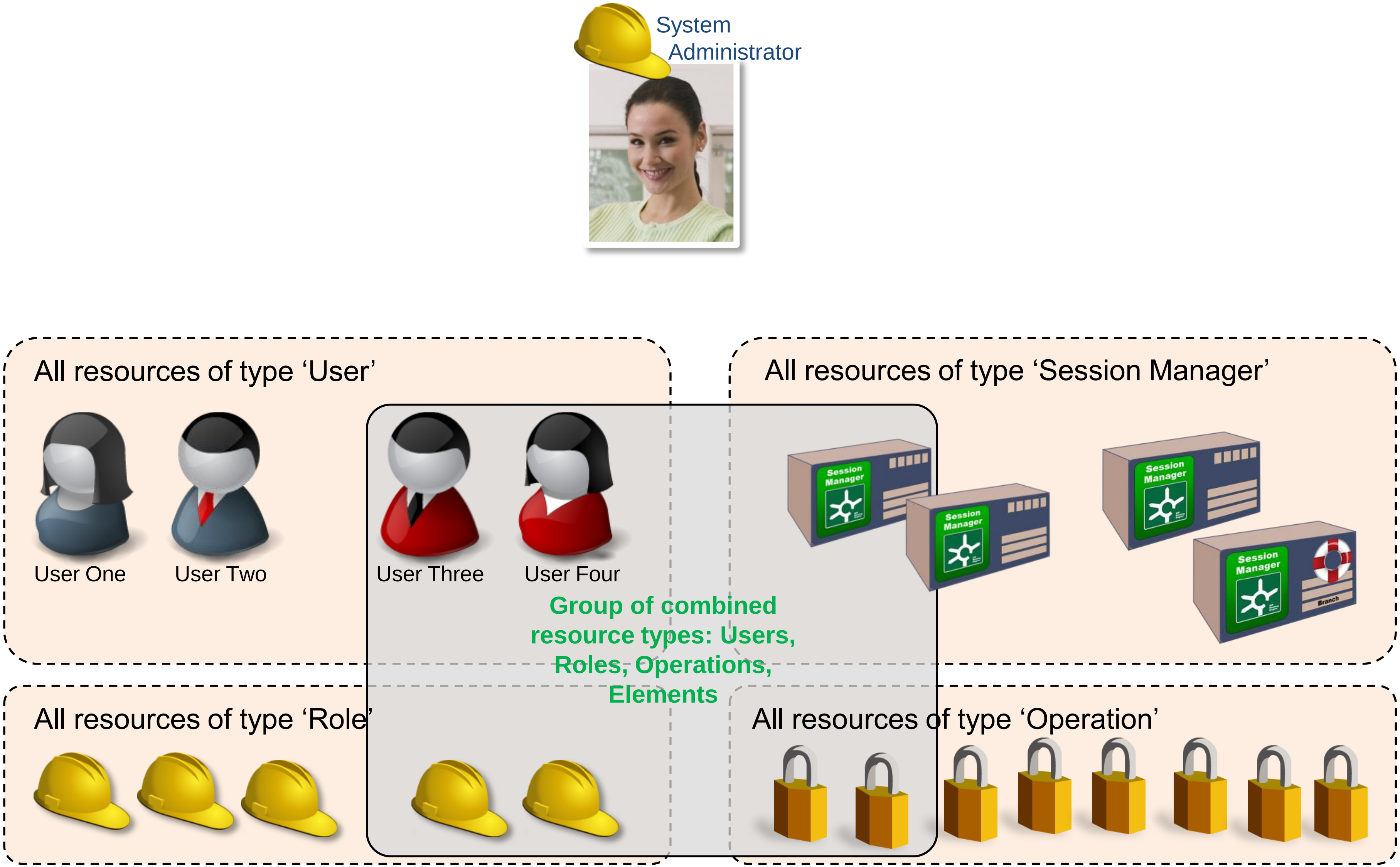
All resources of type ‘Role’

All resources of type ‘Operation’

SMGR Groups – Subsets of Resources



SMGR Groups – Can be Combinations of Resources



System Administrator

All resources of type ‘User’

User One

User Two

User Three

User Four

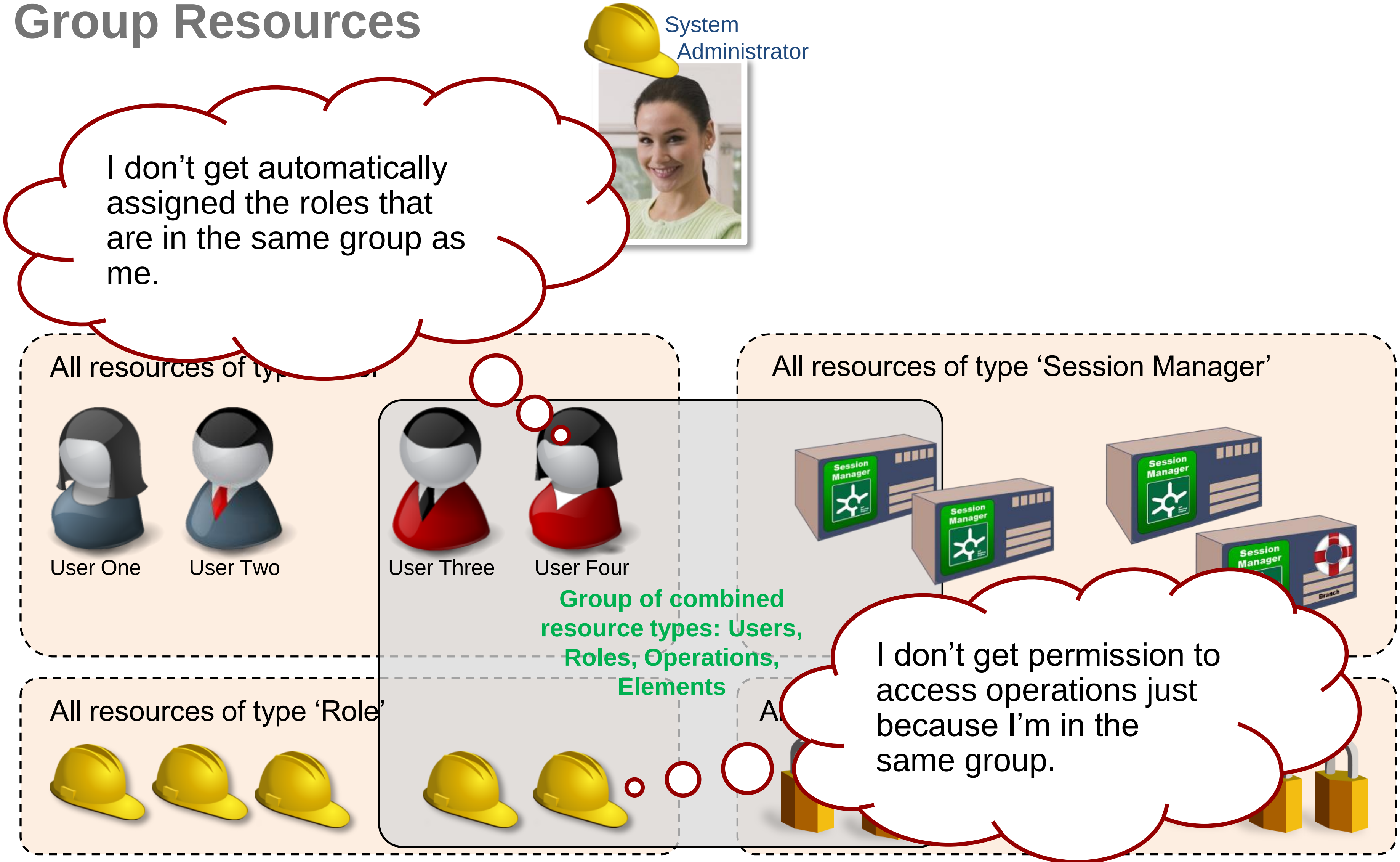
All resources of type ‘Session Manager’

Group of combined resource types: Users, Roles, Operations, Elements

All resources of type ‘Role’

All resources of type ‘Operation’

Being in a Group does not Enable Permissions on Other Group Resources



System Administrator

I don't get automatically assigned the roles that are in the same group as me.

All resources of typ

User One

User Two

User Three

User Four

All resources of type 'Session Manager'

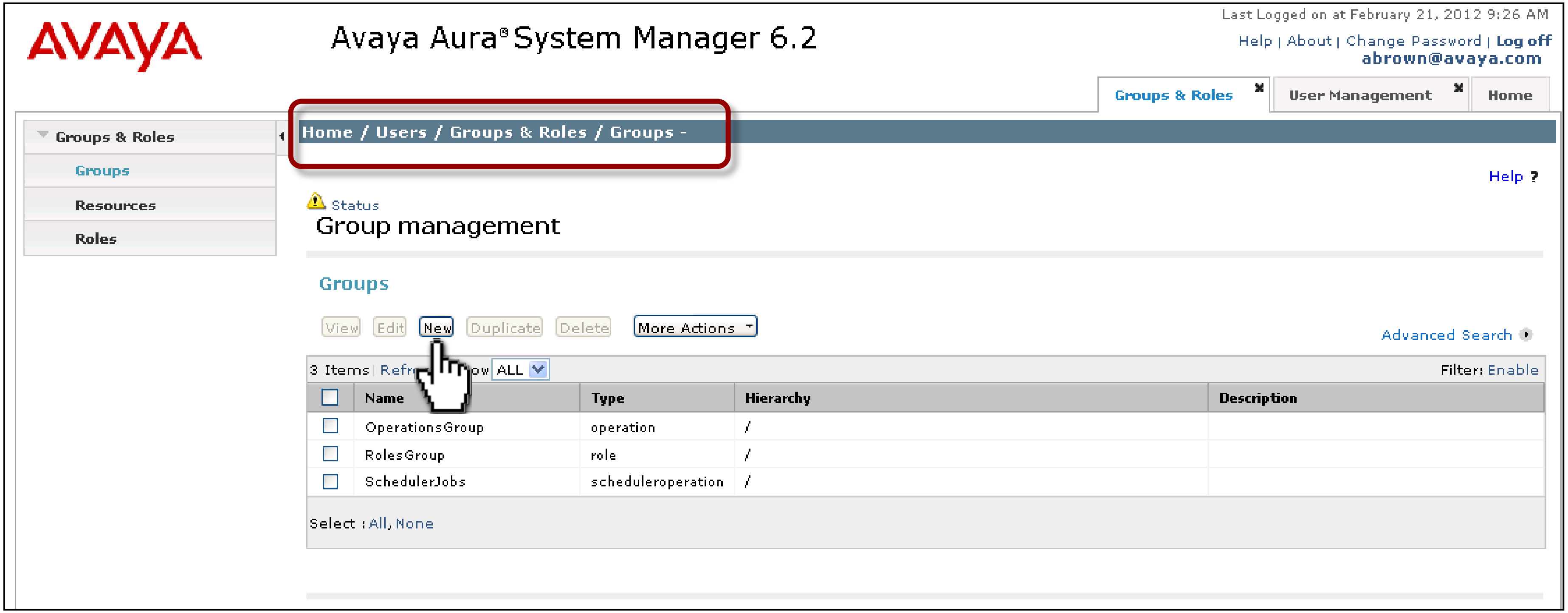
Group of combined resource types: Users, Roles, Operations, Elements

All resources of type 'Role'

A

I don't get permission to access operations just because I'm in the same group.

Creating a Group



Last Logged on at February 21, 2012 9:26 AM

Help | About | Change Password | Log off

abrown@avaya.com

Avaya Aura® System Manager 6.2

Home / Users / Groups & Roles / Groups -

Status

Group management

Groups

3 Items | Refresh | Show ALL

Filter: Enable

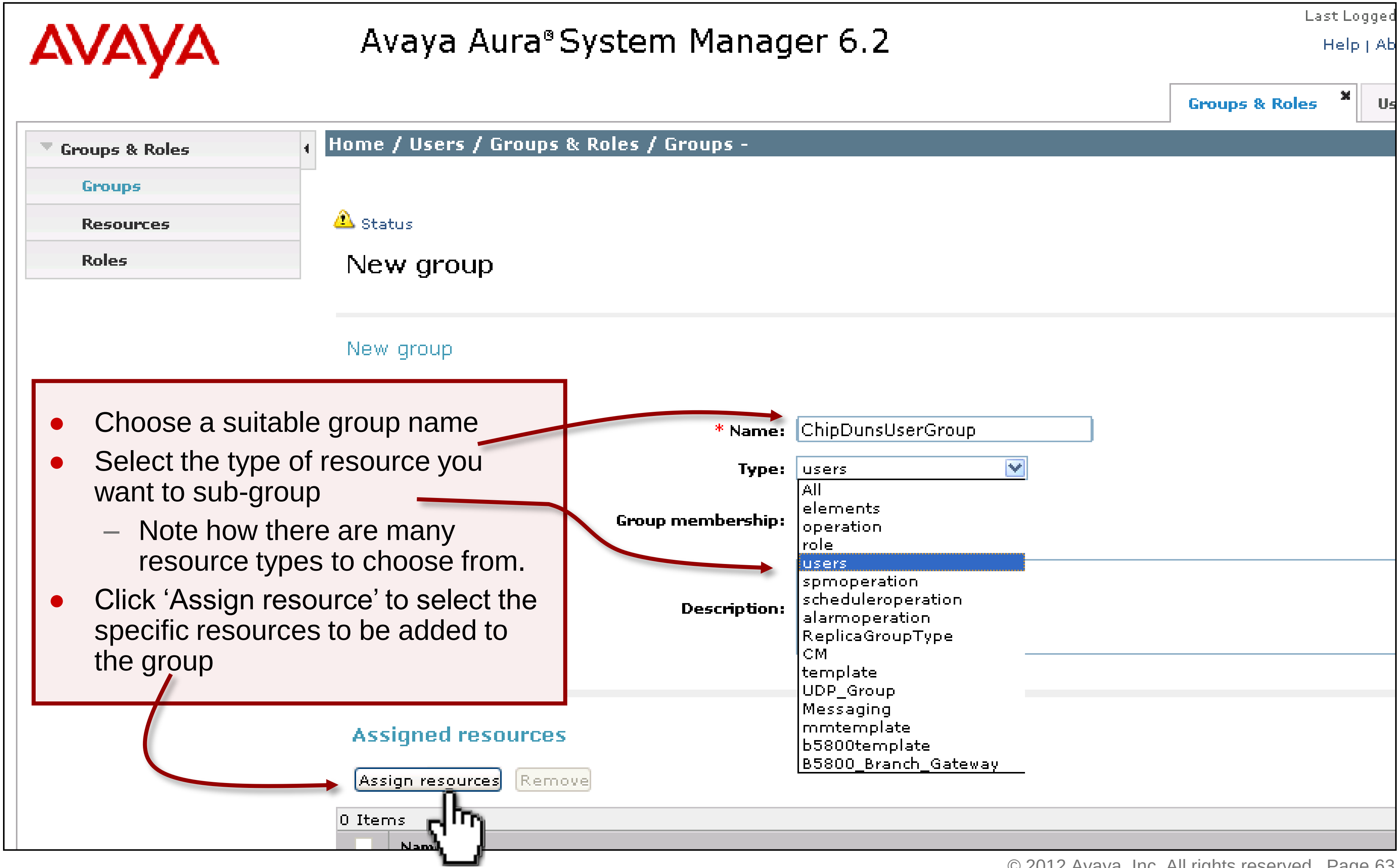
□	Name	Type	Hierarchy	Description
□	OperationsGroup	operation	/	
□	RolesGroup	role	/	
□	SchedulerJobs	scheduleroperation	/	

Select : All, None

To create a new group…

- Navigate to Home > Users > Groups & Roles > Groups
- Click 'New'
- The New Group screen will be displayed

Creating a Group (continued)

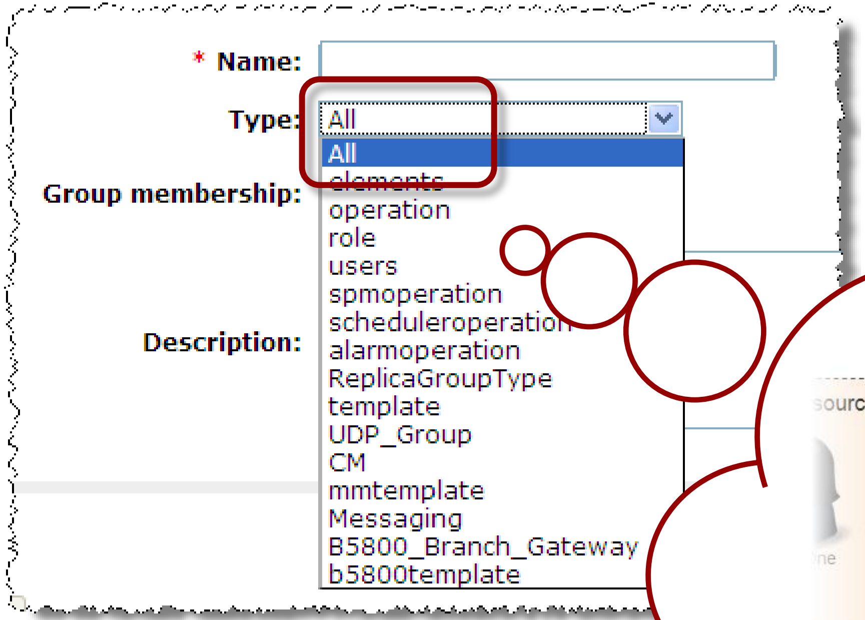


* Name: ChipDunsUserGroup

Type: users

- Choose a suitable group name
- Select the type of resource you want to sub-group
  - Note how there are many resource types to choose from.
- Click ‘Assign resource’ to select the specific resources to be added to the group

Creating a Group of Different Resource Types

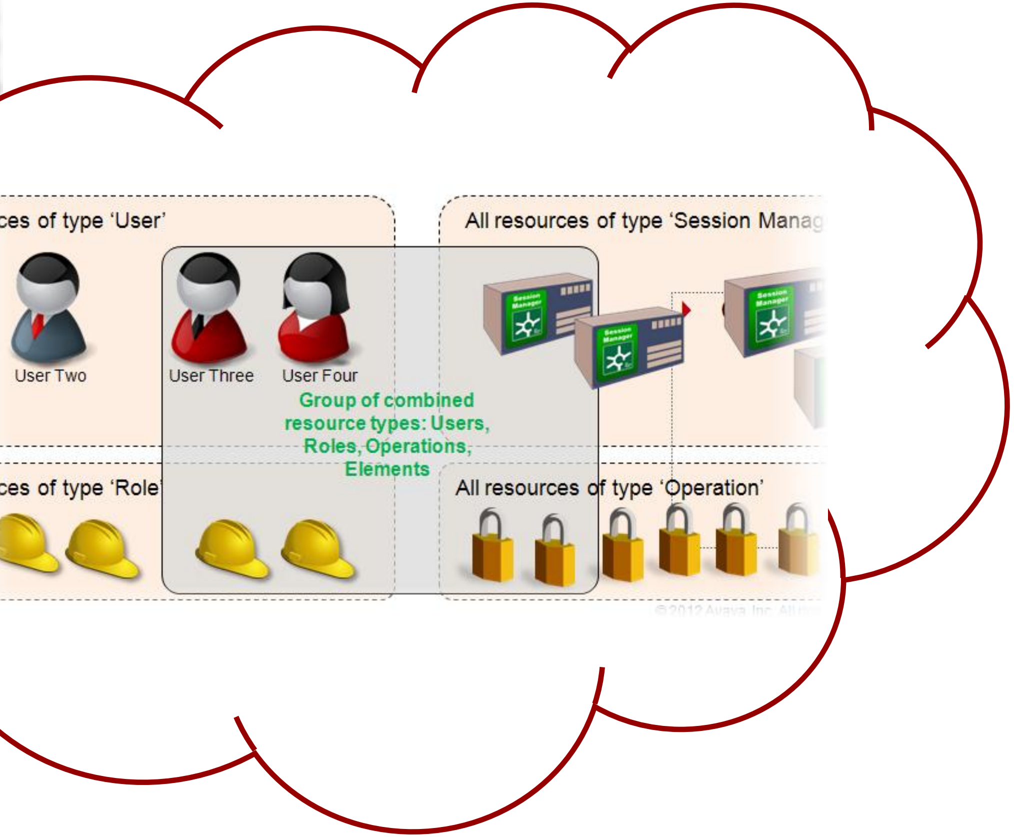


* Name:

Type: All

Group membership:

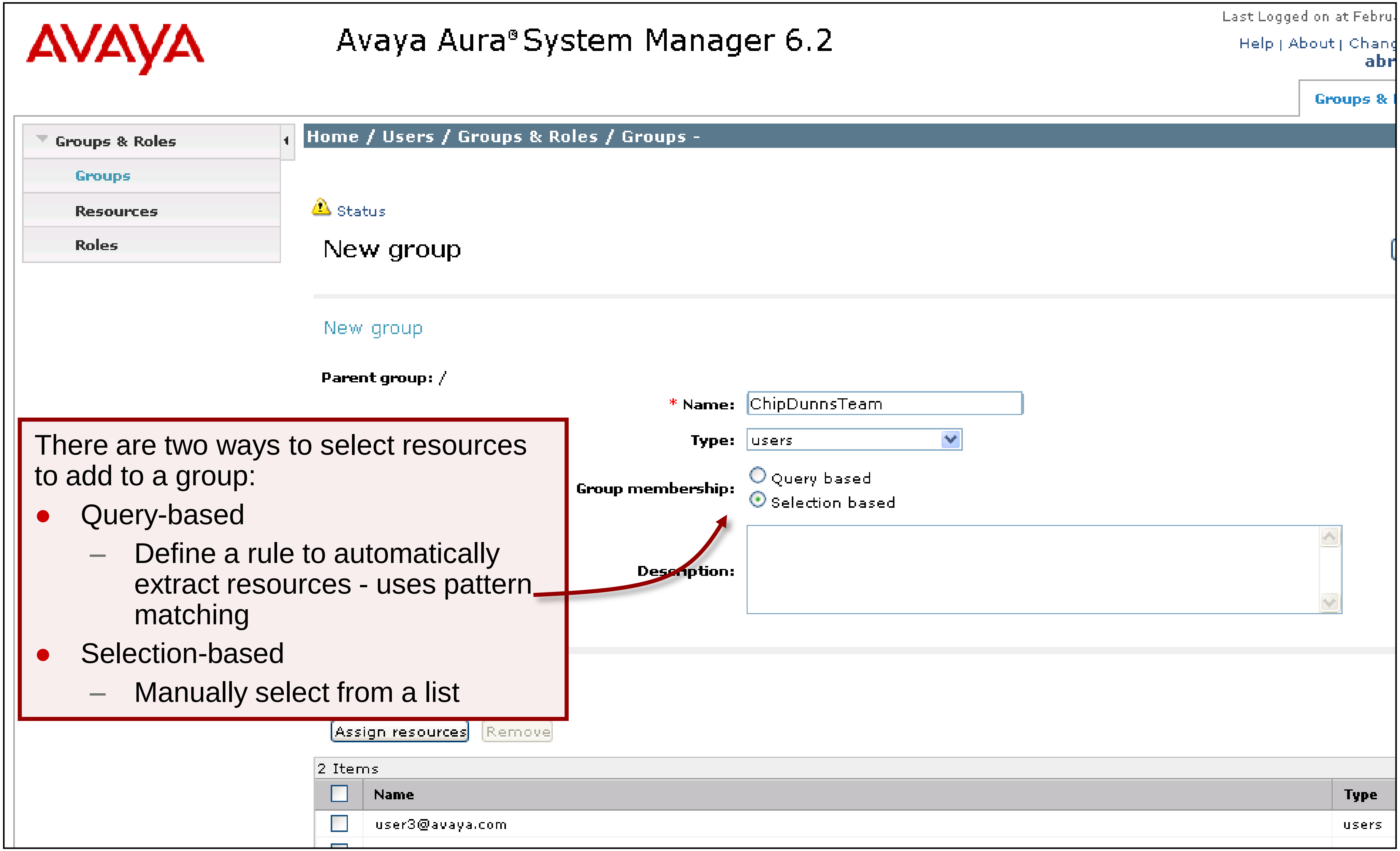
Description:



sources of type 'User'
ne
User Two
User Three
User Four
All resources of type 'Session Manag
Session Manager
Group of combined resource types: Users, Roles, Operations, Elements
sources of type 'Role'
All resources of type 'Operation'

- To create a group that includes different types of resource, select All from the drop down list.

Adding Resources for a Group: Query or Selection?



Home / Users / Groups & Roles / Groups -

Status

New group

New group

Parent group: /

* Name: ChipDunnsTeam

Type: users

Group membership: ○ Query based ● Selection based

Description:

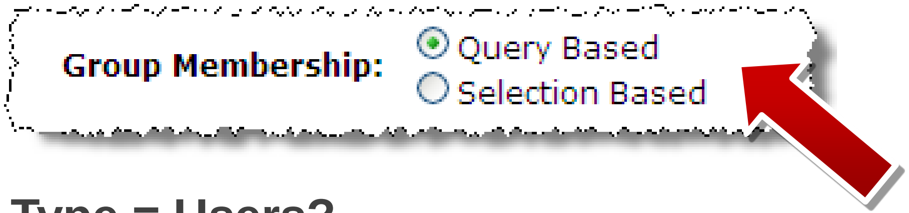
2 Items

□	Name	Type
□	user3@avaya.com	users

There are two ways to select resources to add to a group:

- Query-based
  - Define a rule to automatically extract resources - uses pattern matching
- Selection-based
  - Manually select from a list

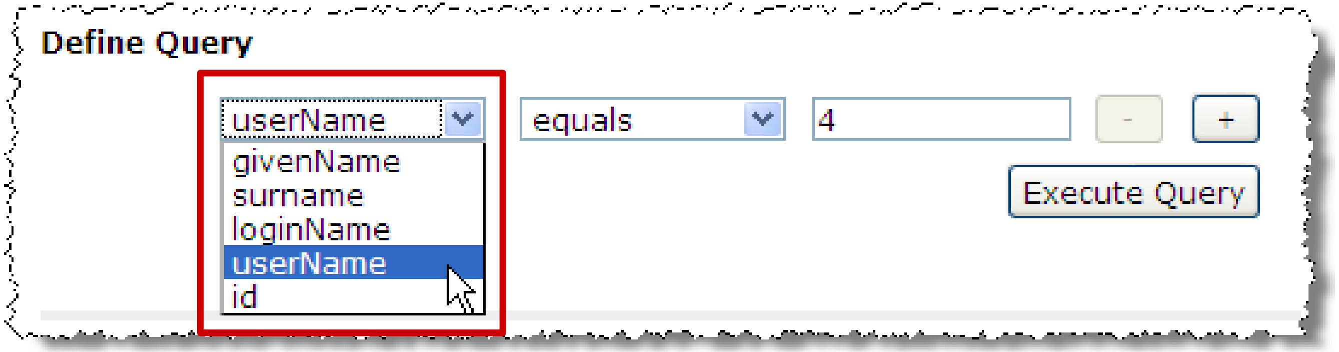
Adding Resources for a Group, Using a Query



Group Membership: ● Query Based ○ Selection Based

- To execute a query you must be able to formulate a pattern that describes which resources you want in the group.
  - E.g. All users who’s userName (extension) starts with a 4

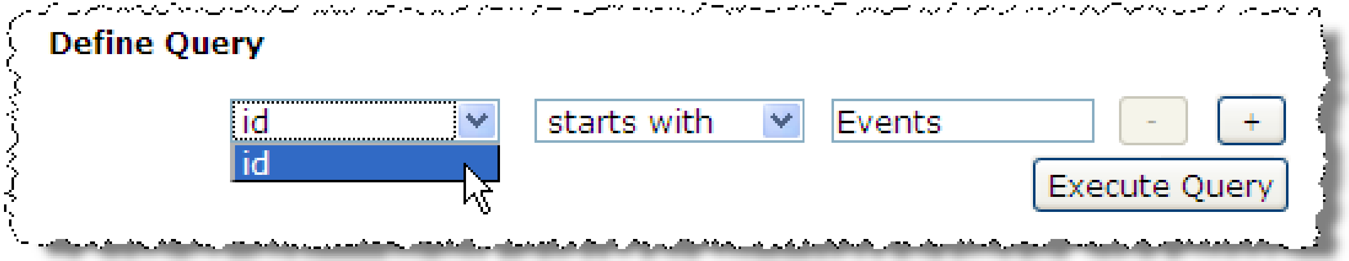
Type = Users?



Define Query

userName equals 4

Type = Operations?

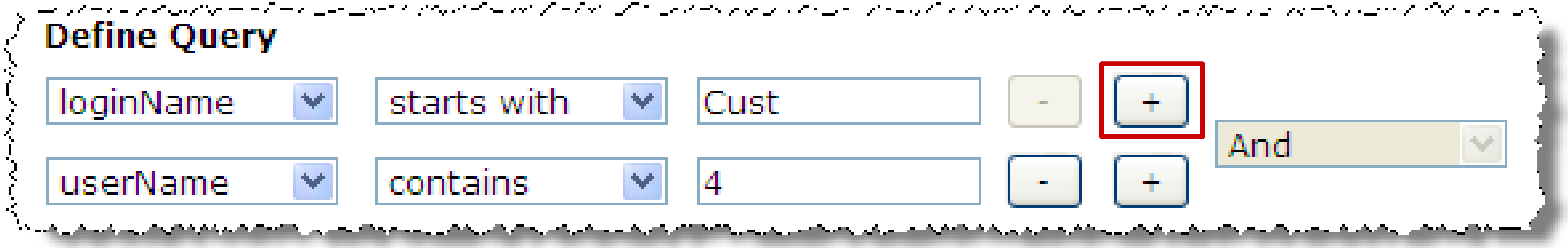


Define Query

id starts with Events

Complex Queries

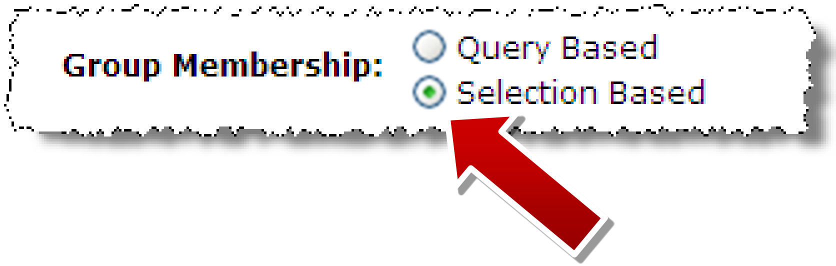
- Build complex queries using the + button to add multiple conditions
- To see the contents of a query defined group, you'll need to execute the query
  - Helpful to think of a query based group as being a description, rather than a discrete set of items



Define Query

loginName	starts with	Cust	-	+	And
userName	contains	4	-	+	

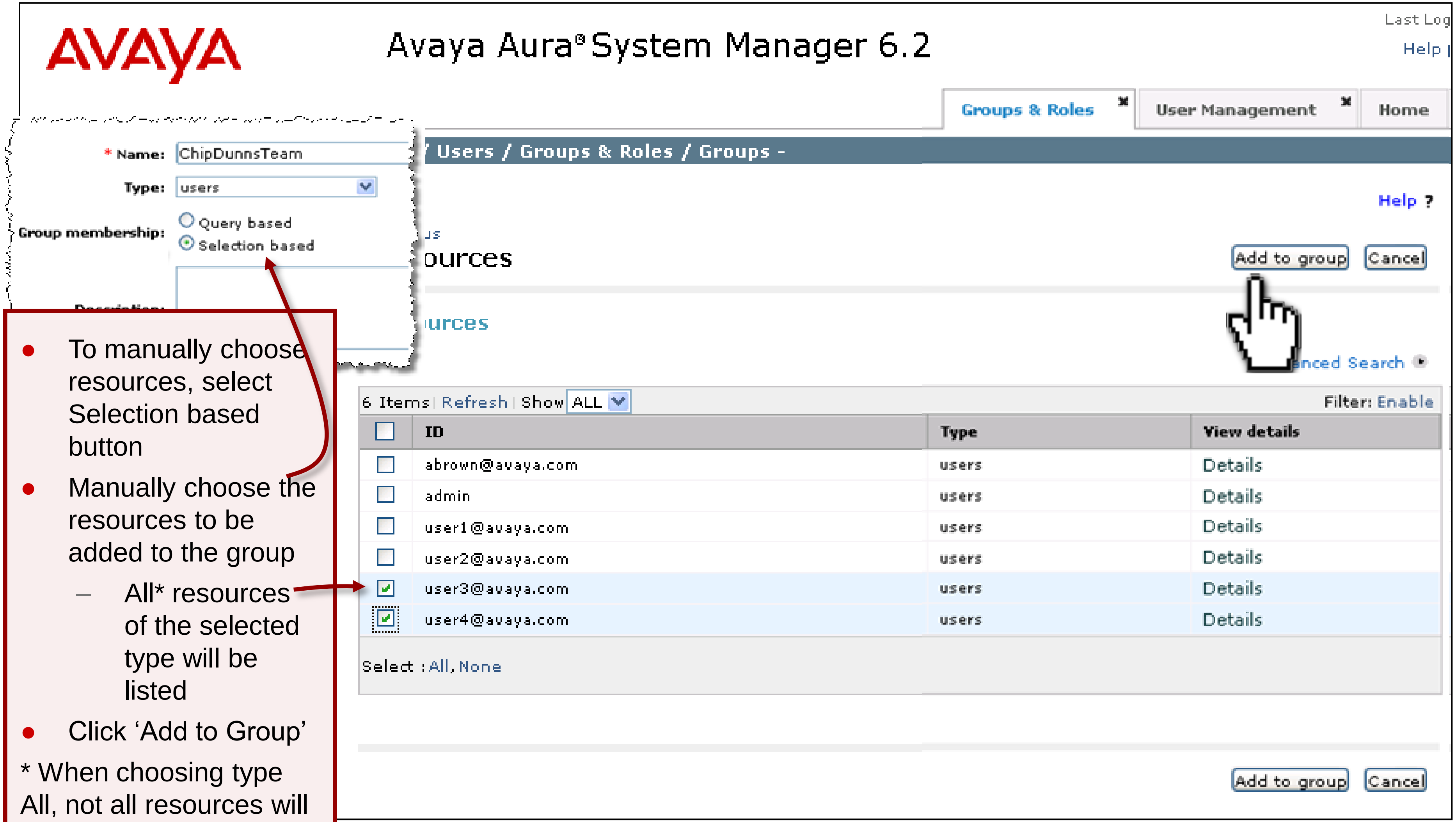
Adding Resources for a Group, Using Manual Selection



Group Membership: ○ Query Based ● Selection Based

- Selection based is conceptually much simpler but perhaps more time consuming
  - Manually select from a list

Manually Selecting Resources for a Group



Avaya Aura® System Manager 6.2

* Name: ChipDunnsTeam

Type: users

Group membership: ○ Query based ● Selection based

Description:

6 Items | Refresh | Show ALL   Filter: Enable

□	ID	Type	View details
□	abrown@avaya.com	users	Details
□	admin	users	Details
□	user1@avaya.com	users	Details
□	user2@avaya.com	users	Details
☑	user3@avaya.com	users	Details
☑	user4@avaya.com	users	Details

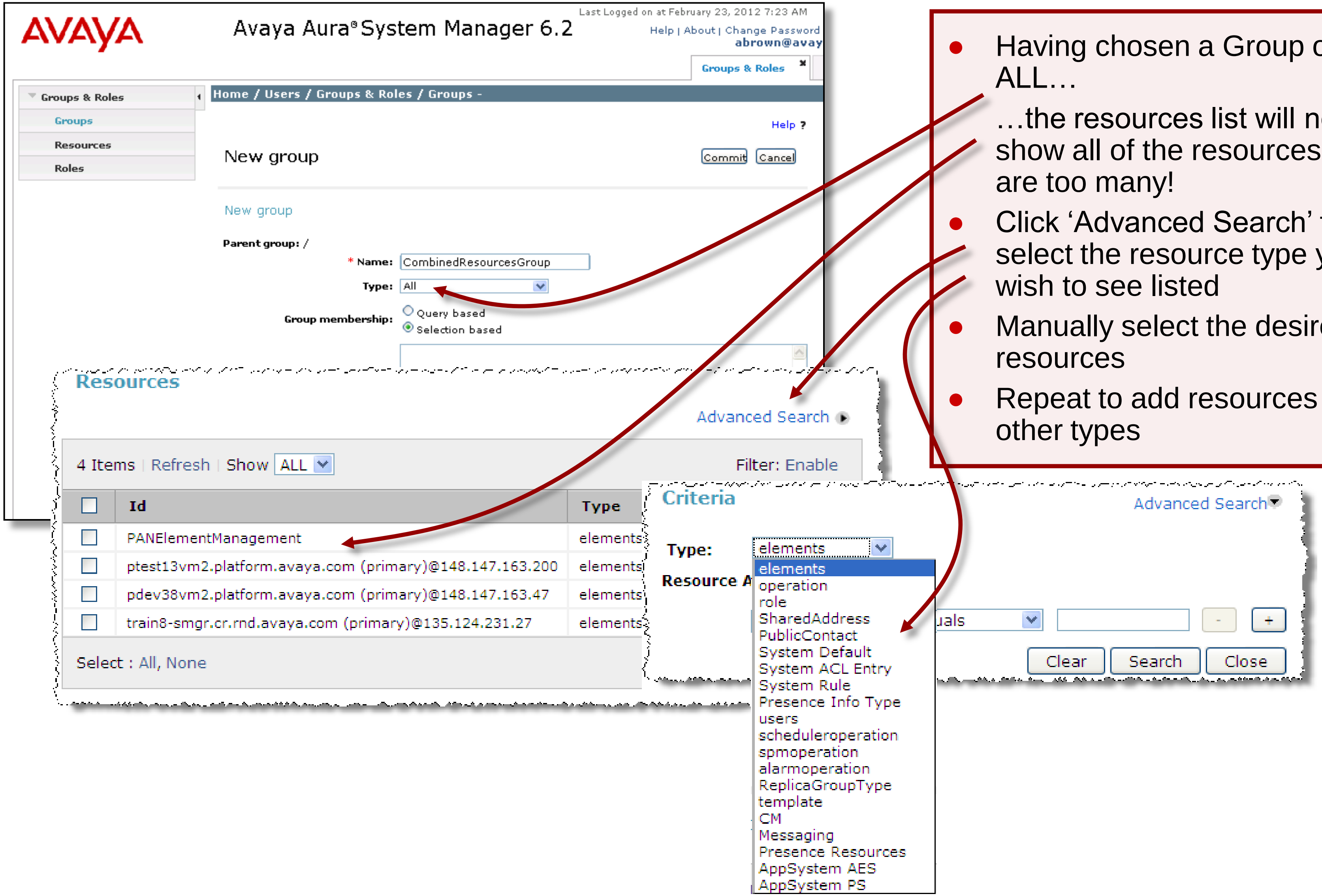
Select : All, None

Add to group Cancel

- To manually choose resources, select Selection based button
- Manually choose the resources to be added to the group
  - All* resources of the selected type will be listed
- Click 'Add to Group'

* When choosing type All, not all resources will be listed. See next slide.

Manually Selecting Resources for a Group – All types?



Last Logged on at February 23, 2012 7:23 AM

Avaya Aura® System Manager 6.2

Help | About | Change Password
abrown@avay

Groups & Roles

Home / Users / Groups & Roles / Groups -

New group

New group

Parent group: /

* **Name:** CombinedResourcesGroup

Type: All

Group membership: ○ Query based ● Selection based

Resources

Advanced Search

4 Items | Refresh | Show ALL | Filter: Enable

□	Id	Type
□	PANElementManagement	elements
□	ptest13vm2.platform.avaya.com (primary)@148.147.163.200	elements
□	pdev38vm2.platform.avaya.com (primary)@148.147.163.47	elements
□	train8-smgr.cr.rnd.avaya.com (primary)@135.124.231.27	elements

Select : All, None

Criteria

Advanced Search

Type: elements

Resource A

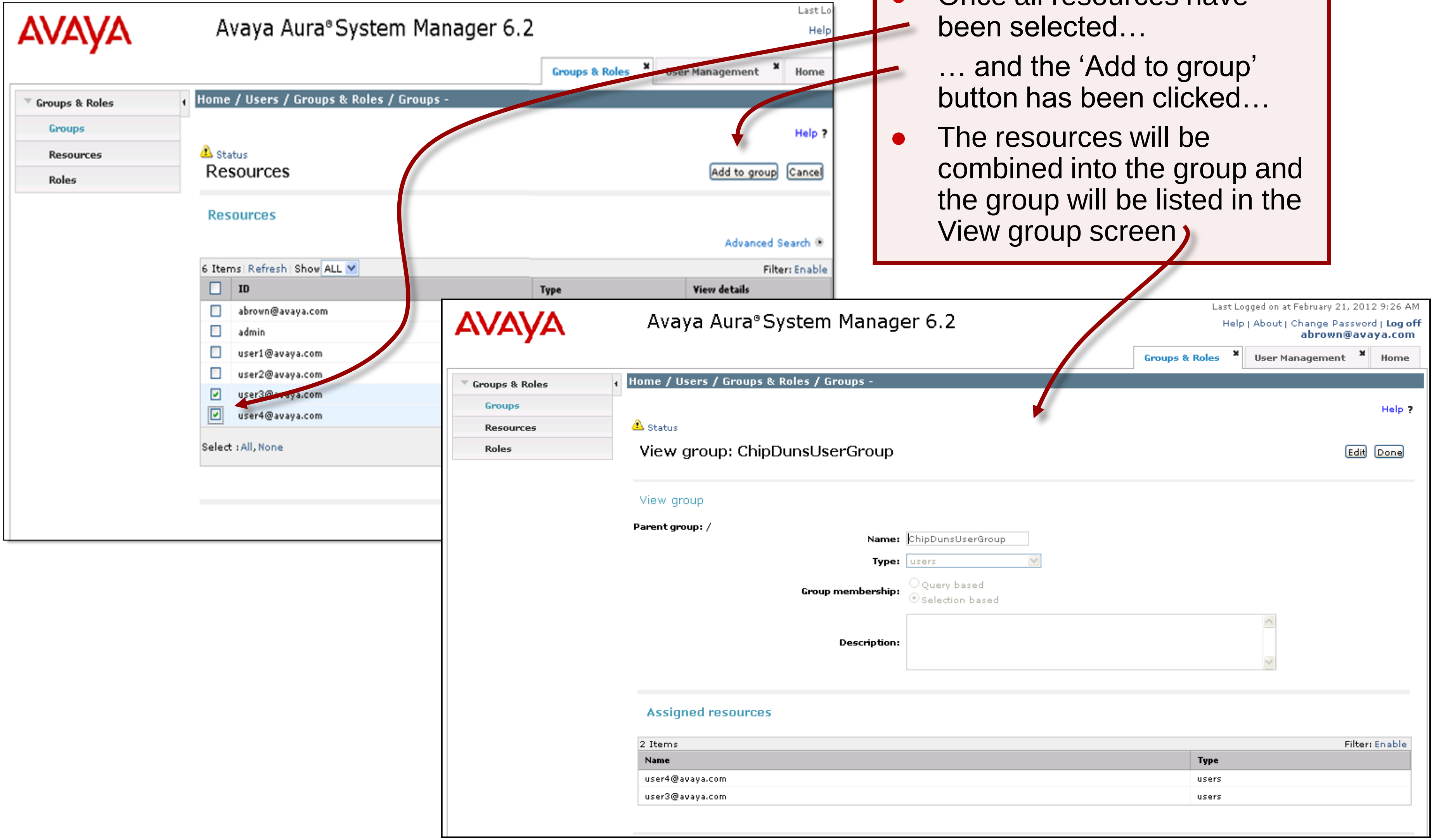
- Having chosen a Group of type ALL…

  …the resources list will not show all of the resources – there are too many!
- Click 'Advanced Search' then select the resource type you wish to see listed
- Manually select the desired resources
- Repeat to add resources of other types

Finishing the Group

- Once all resources have been selected…

  … and the 'Add to group' button has been clicked…
- The resources will be combined into the group and the group will be listed in the View group screen



Resources

	ID	Type	View details
□	abrown@avaya.com		
□	admin		
□	user1@avaya.com		
□	user2@avaya.com		
☑	user3@avaya.com		
☑	user4@avaya.com		

Select : All, None
AVAYA
Avaya Aura® System Manager 6.2
Last Logged on at February 21, 2012 9:26 AM
Help | About | Change Password | Log off
abrown@avaya.com
Groups & Roles
User Management
Home
Groups & Roles
Groups
Resources
Roles
Home / Users / Groups & Roles / Groups -
Help ?
Status

View group: ChipDunsUserGroup

Parent group: /

Name: ChipDunsUserGroup

Type: users

Group membership: ○ Query based ● Selection based

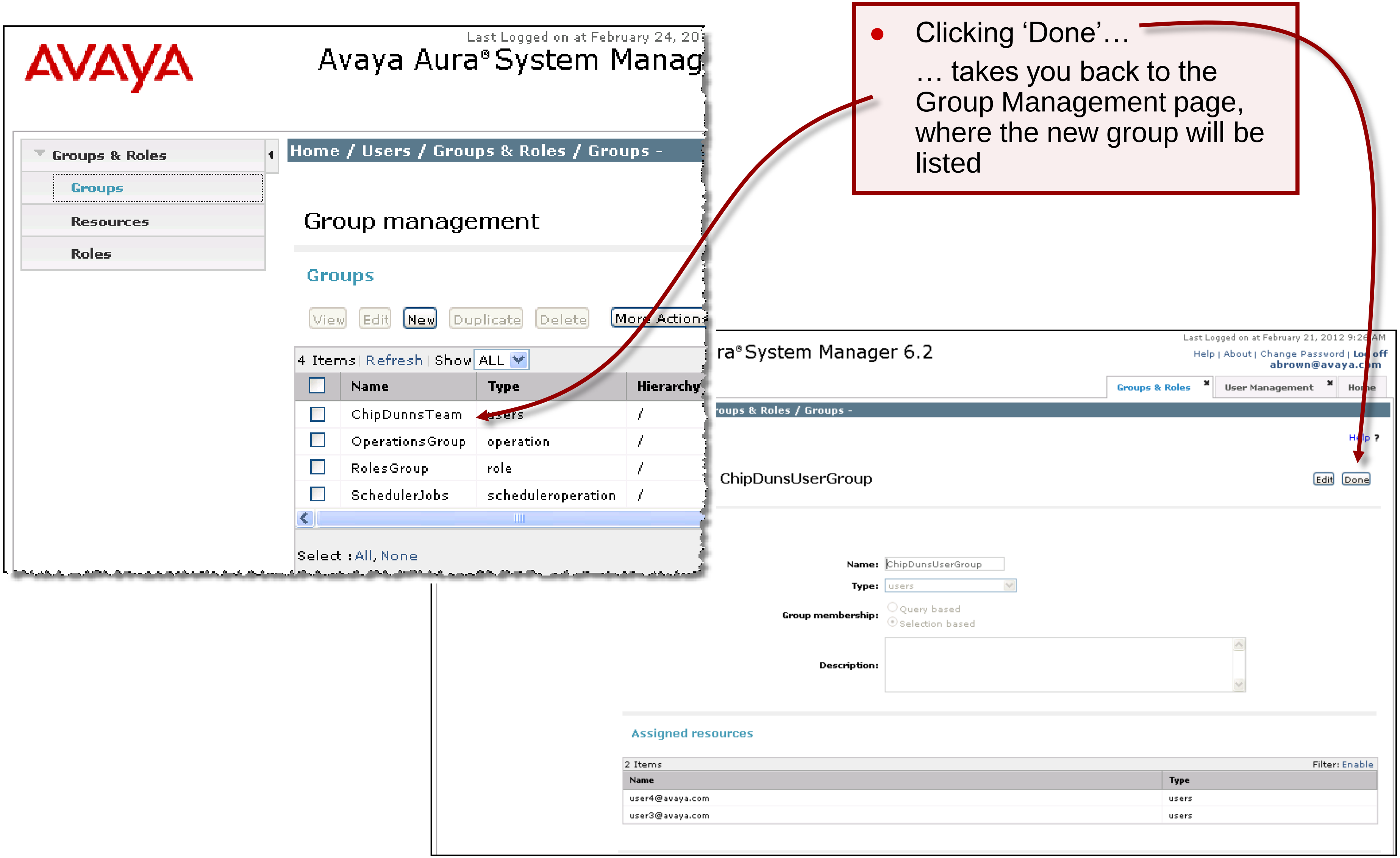
Description:

Assigned resources

2 Items — Filter: Enable

Name	Type
user4@avaya.com	users
user3@avaya.com	users

Finishing the Group (continued)



Last Logged on at February 24, 20

Avaya Aura® System Manag

Home / Users / Groups & Roles / Groups -

Group management

Groups

4 Items | Refresh | Show ALL

□	Name	Type	Hierarchy
□	ChipDunnsTeam	users	/
□	OperationsGroup	operation	/
□	RolesGroup	role	/
□	SchedulerJobs	scheduleroperation	/

Select : All, None

Last Logged on at February 21, 2012 9:26 AM

ra® System Manager 6.2

roups & Roles / Groups -

ChipDunsUserGroup

Name: ChipDunsUserGroup

Type: users

Group membership: ○ Query based ● Selection based

Description:

Assigned resources

2 Items   Filter: Enable

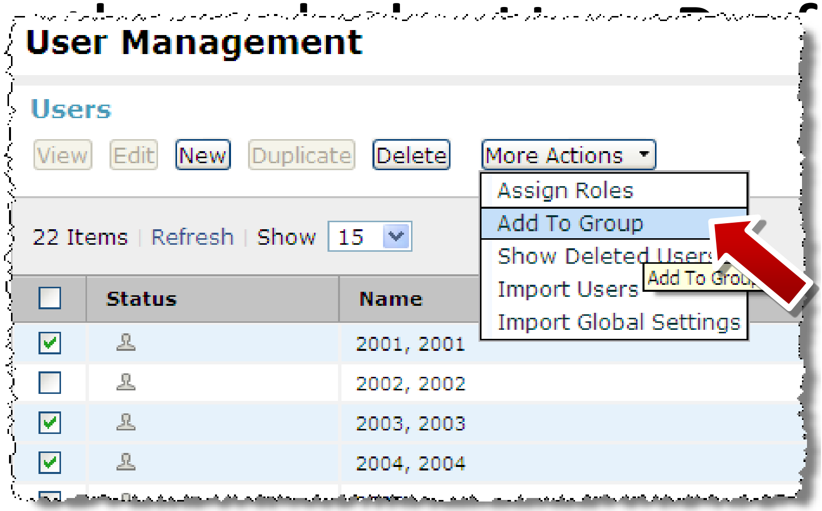
Name	Type
user4@avaya.com	users
user3@avaya.com	users

- Clicking 'Done'…

  … takes you back to the Group Management page, where the new group will be listed

Adding Users to a Group: Two Methods

- Users may also be subsequently added to a group

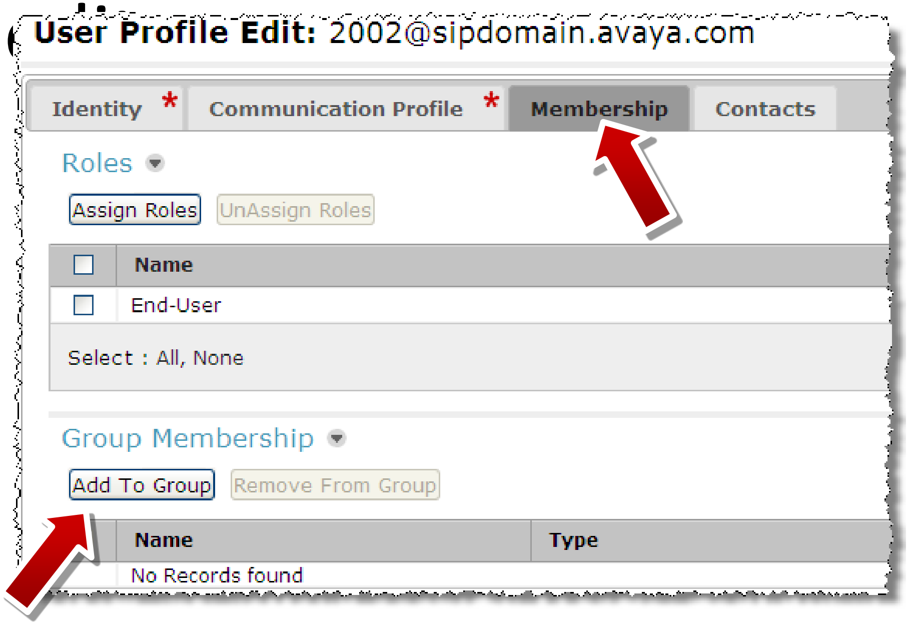


User Management

Users

22 Items | Refresh | Show 15

☐	Status	Name
☑		2001, 2001
☐		2002, 2002
☑		2003, 2003
☑		2004, 2004



User Profile Edit: 2002@sipdomain.avaya.com

Roles

☐	Name
☐	End-User

Select : All, None

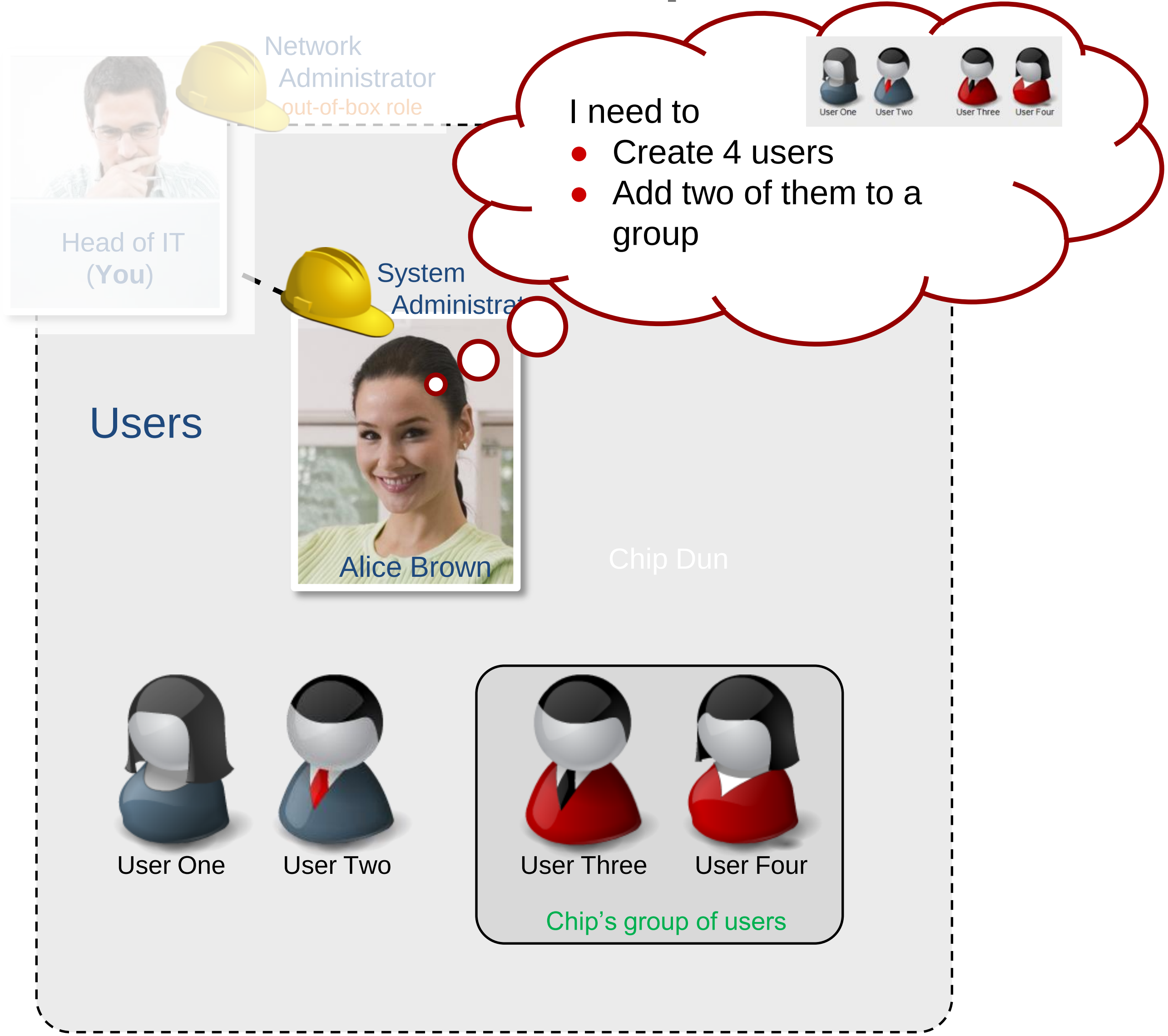
Group Membership

	Name	Type
	No Records found	

Add several users to group at once
(User Management screen)

Add user individually
(Edit user profile)

Practical: Create a Group of Users



I need to

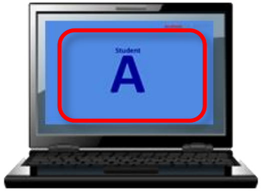
- Create 4 users
- Add two of them to a group

Exercise: Create a Group of Users

Objective & Outcome
The objective is to learn how to use groups to specify fine grained RBAC permissions. In this exercise, you will create a group of users and add them to a group. (In the next exercise, you will use the group in defining a custom role.) When done, you will see the list of groups, including the new group with its two users.

1. Create 4 new users that can be added to a group. (Log back in as System Admin – abrown)
   - Navigate to: Home > User Management > Manage Users. Click button ‘New’
   - Identity tab: Enter only the mandatory data – choose your own names, etc. Repeat 4 times.
2. Create Group of users for Chip’s team
   - Navigate to: Home > Groups & Roles. Click ‘Groups’ in the menu. Click button ‘***New***’
   - In the New Group screen enter the Name ‘**ChipDunnsTeam**’. Set Group Membership radio button to ‘***Selection based***’. Click button ‘***Assign Resources***’. The Resources screen now lists all resources of type User.
   - Select 2 of the new users. Click ‘***Add to group***’. From New Group screen click ‘***Commi****t*’.
3. Check the Group of users
   - Check that the new group appears in the list of groups
   - Edit the group to check that it contains only two users – the same two you added a moment ago

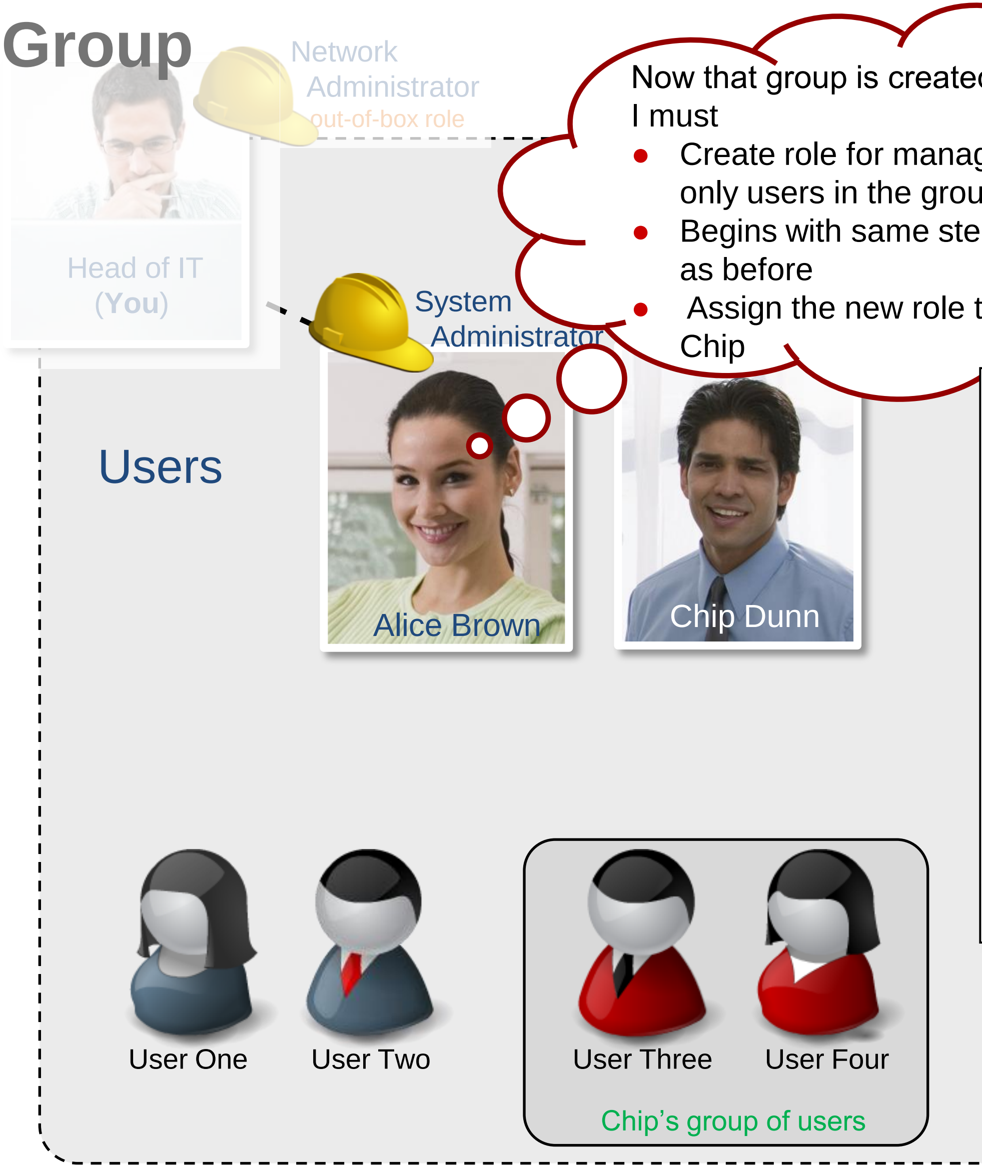
Individual Exercise – both students can work simultaneously



Student A

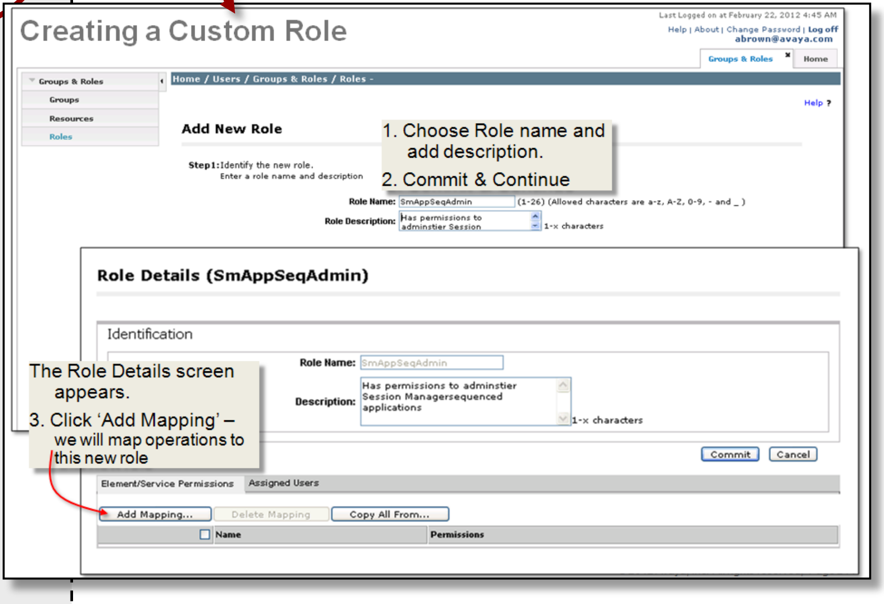
Student B

Create a Role with Permissions Only for Resources in a Group



Now that group is created…
I must

- Create role for managing only users in the group
- Begins with same steps as before
- Assign the new role to Chip



Creating a Custom Role

Last Logged on at February 22, 2012 4:45 AM
Help | About | Change Password | Log off
abrown@avaya.com
Groups & Roles
Home
Groups & Roles
Groups
Resources
Roles
Home / Users / Groups & Roles / Roles -
Help ?

Add New Role

Step1:Identify the new role.
Enter a role name and description

1. Choose Role name and add description.
2. Commit & Continue

Role Name: SmAppSeqAdmin (1-26) (Allowed characters are a-z, A-Z, 0-9, - and _)

Role Description: Has permissions to adminstier Session 1-x characters

Role Details (SmAppSeqAdmin)

Identification

Role Name: SmAppSeqAdmin

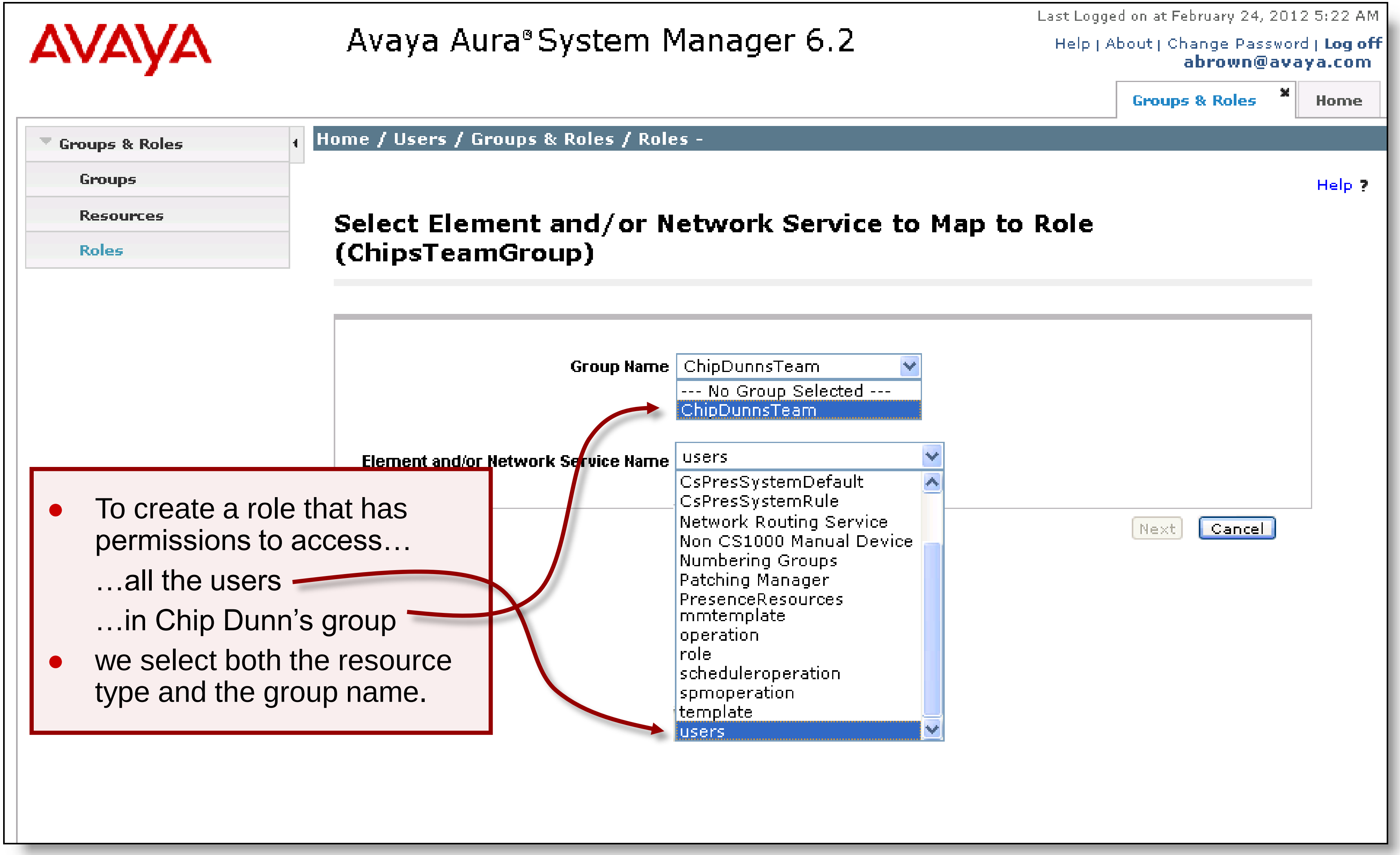
Description: Has permissions to adminstier Session Managersequenced applications 1-x characters

The Role Details screen appears.

3. Click 'Add Mapping' – we will map operations to this new role

- Need to understand Attributes and Actions

Elements and Network Services



Avaya Aura® System Manager 6.2

Last Logged on at February 24, 2012 5:22 AM

Help | About | Change Password | Log off

abrown@avaya.com

Groups & Roles
Home
Groups & Roles
Groups
Resources
Roles
Home / Users / Groups & Roles / Roles -
Help ?

Select Element and/or Network Service to Map to Role (ChipsTeamGroup)

Group Name: ChipDunnsTeam

- --- No Group Selected ---
- ChipDunnsTeam

Element and/or Network Service Name: users

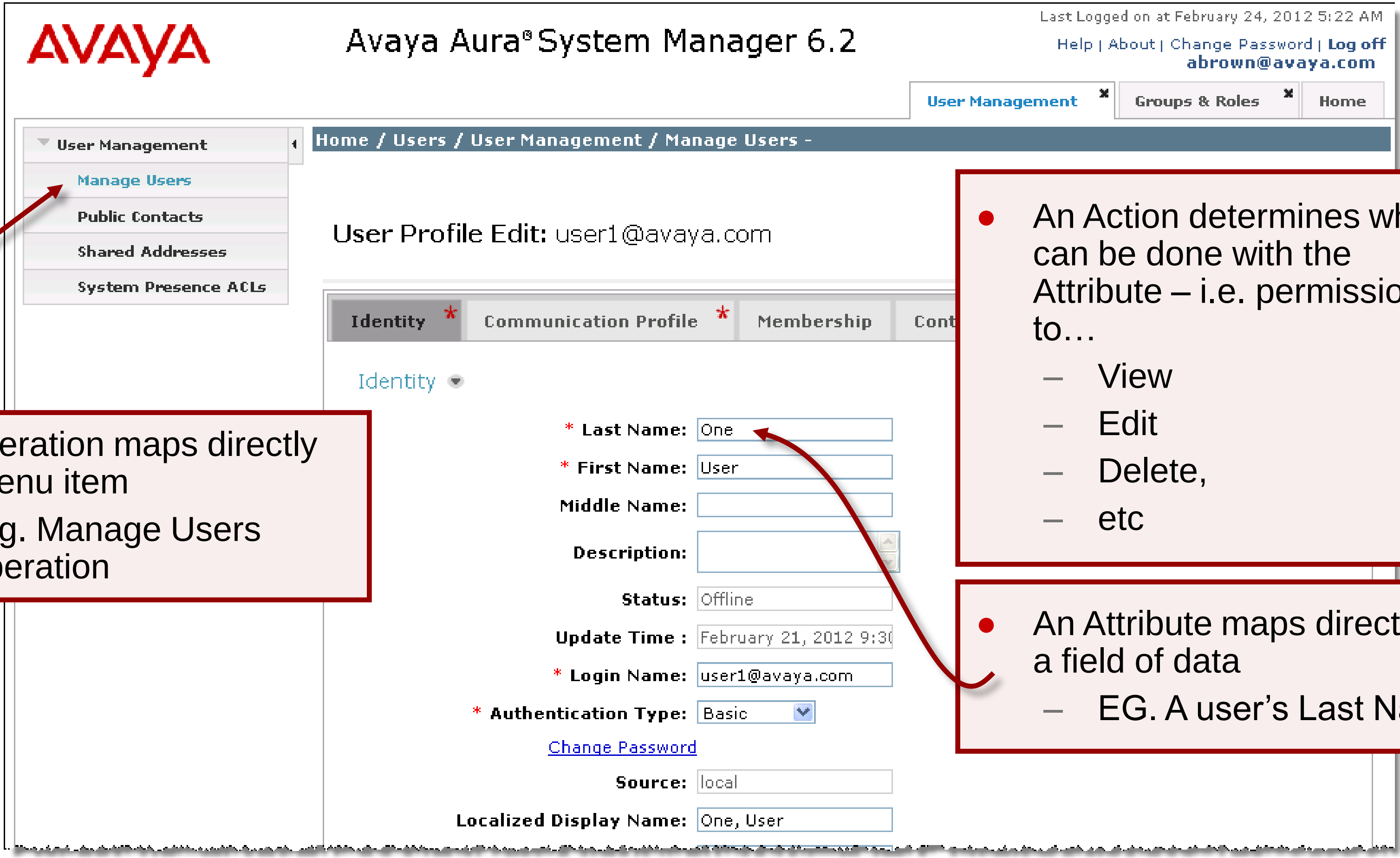
- CsPresSystemDefault
- CsPresSystemRule
- Network Routing Service
- Non CS1000 Manual Device
- Numbering Groups
- Patching Manager
- PresenceResources
- mmtemplate
- operation
- role
- scheduleroperation
- spmoperation
- template
- users

- To create a role that has permissions to access…

  …all the users

  …in Chip Dunn's group
- we select both the resource type and the group name.

Operations, Attributes and Actions



User Profile Edit: user1@avaya.com

Identity

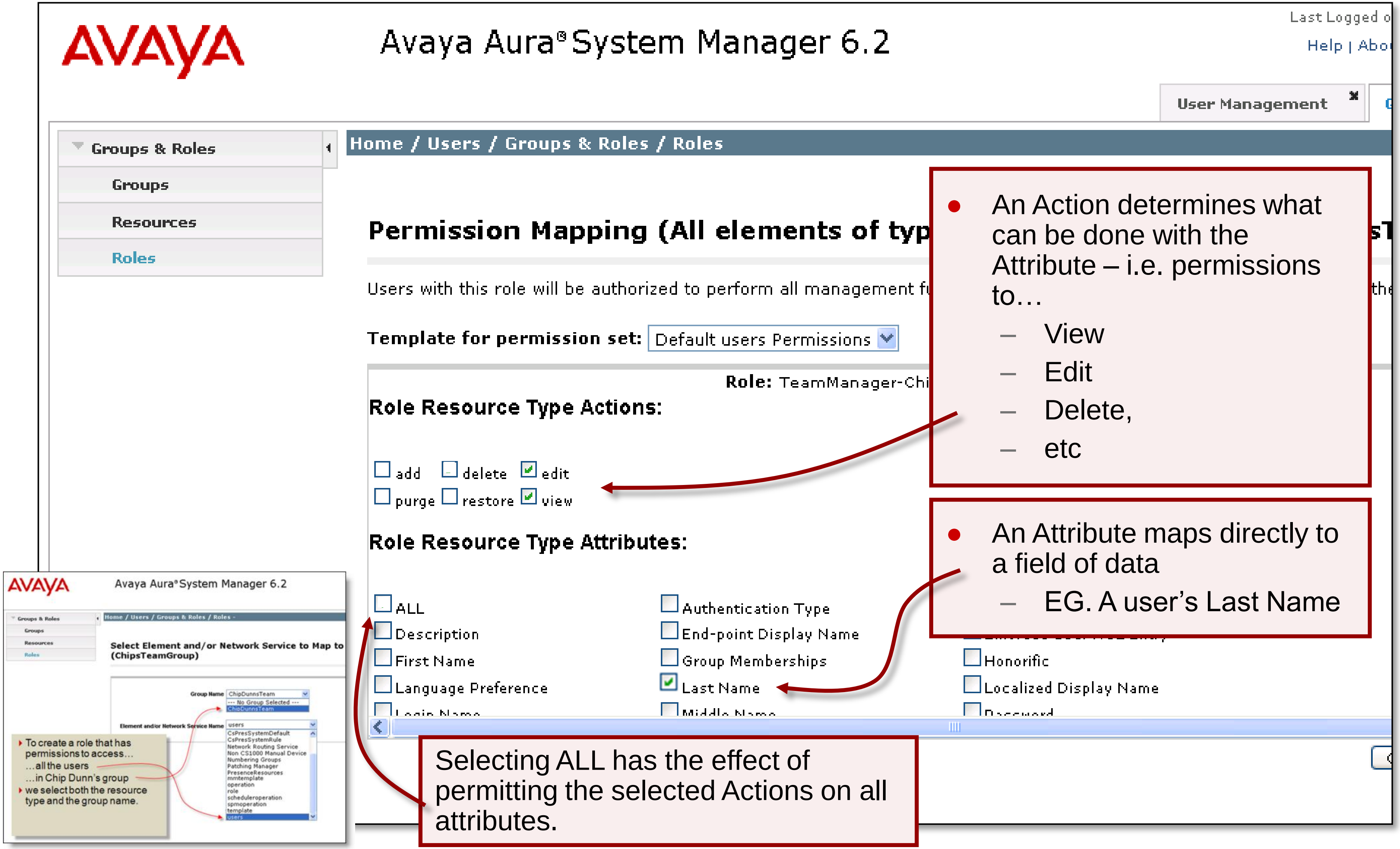
* Last Name:	One
* First Name:	User
Middle Name:	
Description:	
Status:	Offline
Update Time :	February 21, 2012 9:3(
* Login Name:	user1@avaya.com
* Authentication Type:	Basic
Change Password	
Source:	local
Localized Display Name:	One, User

- An Operation maps directly to a menu item
  - E.g. Manage Users operation

- An Action determines what can be done with the Attribute – i.e. permissions to…
  - View
  - Edit
  - Delete,
  - etc

- An Attribute maps directly to a field of data
  - EG. A user’s Last Name

Permissions to Take Action and Change Attributes



Permission Mapping (All elements of typ

Users with this role will be authorized to perform all management f

Template for permission set: Default users Permissions

Role: TeamManager-Chi

Role Resource Type Actions:

□ add □ delete ☑ edit
□ purge □ restore ☑ view

Role Resource Type Attributes:

□ ALL	□ Authentication Type	
□ Description	□ End-point Display Name	
□ First Name	□ Group Memberships	□ Honorific
□ Language Preference	☑ Last Name	□ Localized Display Name
□ Login Name	□ Middle Name	□ Password

- An Action determines what can be done with the Attribute – i.e. permissions to…
  - View
  - Edit
  - Delete,
  - etc

- An Attribute maps directly to a field of data
  - EG. A user's Last Name

Selecting ALL has the effect of permitting the selected Actions on all attributes.

AVAYA
Avaya Aura® System Manager 6.2
Groups & Roles
Groups
Resources
Roles
Home / Users / Groups & Roles / Roles -

Select Element and/or Network Service to Map to (ChipsTeamGroup)

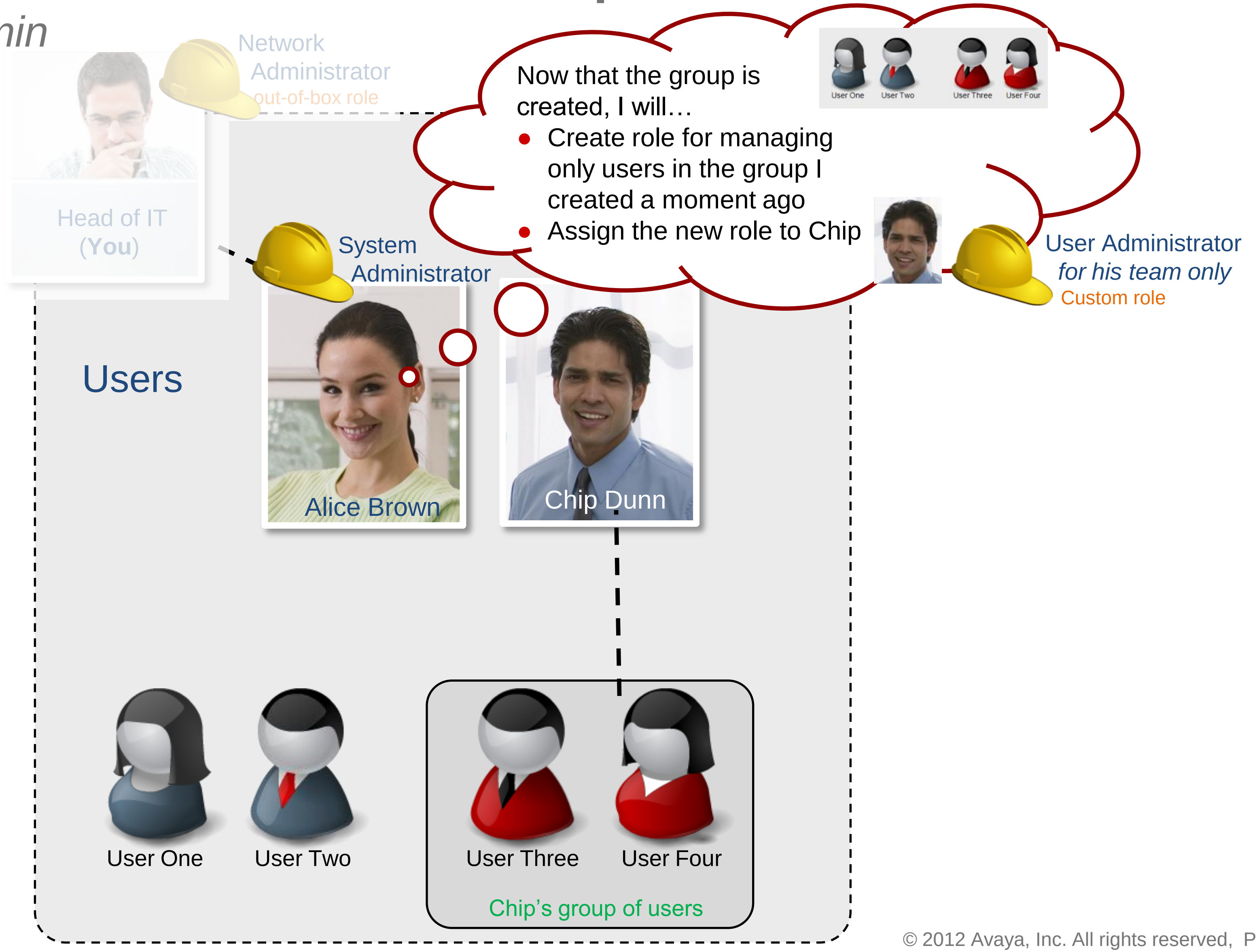
Group Name ChipDunnsTeam
--- No Group Selected ---
ChipDunnsTeam

Element and/or Network Service Name users
CsPresSystemDefault
CsPresSystemRule
Network Routing Service
Non CS1000 Manual Device
Numbering Groups
Patching Manager
PresenceResources
mmtemplate
operation
role
scheduleroperation
spmoperation
template
users

- To create a role that has permissions to access…
  …all the users
  …in Chip Dunn's group
- we select both the resource type and the group name.

Practical: Create Custom 'Group based' Role

User Admin



Now that the group is created, I will…

- Create role for managing only users in the group I created a moment ago
- Assign the new role to Chip

Exercise: Create and Assign a Custom Group-Oriented Role

Objective & Outcome

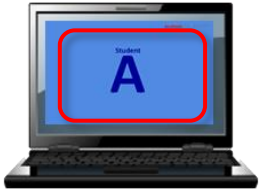
The objective is to learn how to use groups to specify fine grained RBAC permissions. In the previous exercise you created a group of users. In this exercise you will create a custom role that will permit a user to administer only the users in the group. When done, you will log in as the new administrator and should have access only to the users belonging to the group.

1. Create a new role that gives access only to the subset of users in the new group
   - Navigate to: Home > Groups & Roles > Roles. Click button ‘***Add***’
   - Enter new Role Name ‘**AdministratorofChipsTeam**’ and description. Click ***’Commit & Continue’***
   - Click on ***Add Mapping***
   - From the Select Element… screen select ‘**ChipDunnsTeam**’ from the Group Name list.
   - Select ‘**users**’ from the Elements list. Click ‘***Next***’.
   - From the Permission Mapping screen, select all ***Resource Type Actions (add, purge…)***, and the top most ***Role Resource Type Attribute*** ‘**ALL**’, signifying all the subsequent attributes are also selected. Click ‘***Commit’.***
   - From the Role Details screen, check the new mapping has been added and click ‘***Commit’***.

2. Assign the new role to Chip
   - Navigate to: Home > Users > User Management > Manage Users
   - Select **Chip Dunn** from the list of users and click button ‘***Edit’***
   - From ‘Membership’ tab, click button ‘***Assign Roles***’
   - Select role ‘**AdministratorofChipsTeam’** and click ‘***Select*** and then ‘***Commit’.***

3. Check that Chip has access to his team members
   - Log out of **abrown@avaya.com** and log back in as **cdunn@avaya.com** (password Passw0rd!)
   - Navigate to: Home > User Management > Manage Users

Individual Exercise – both students can work simultaneously



Student A

Student B

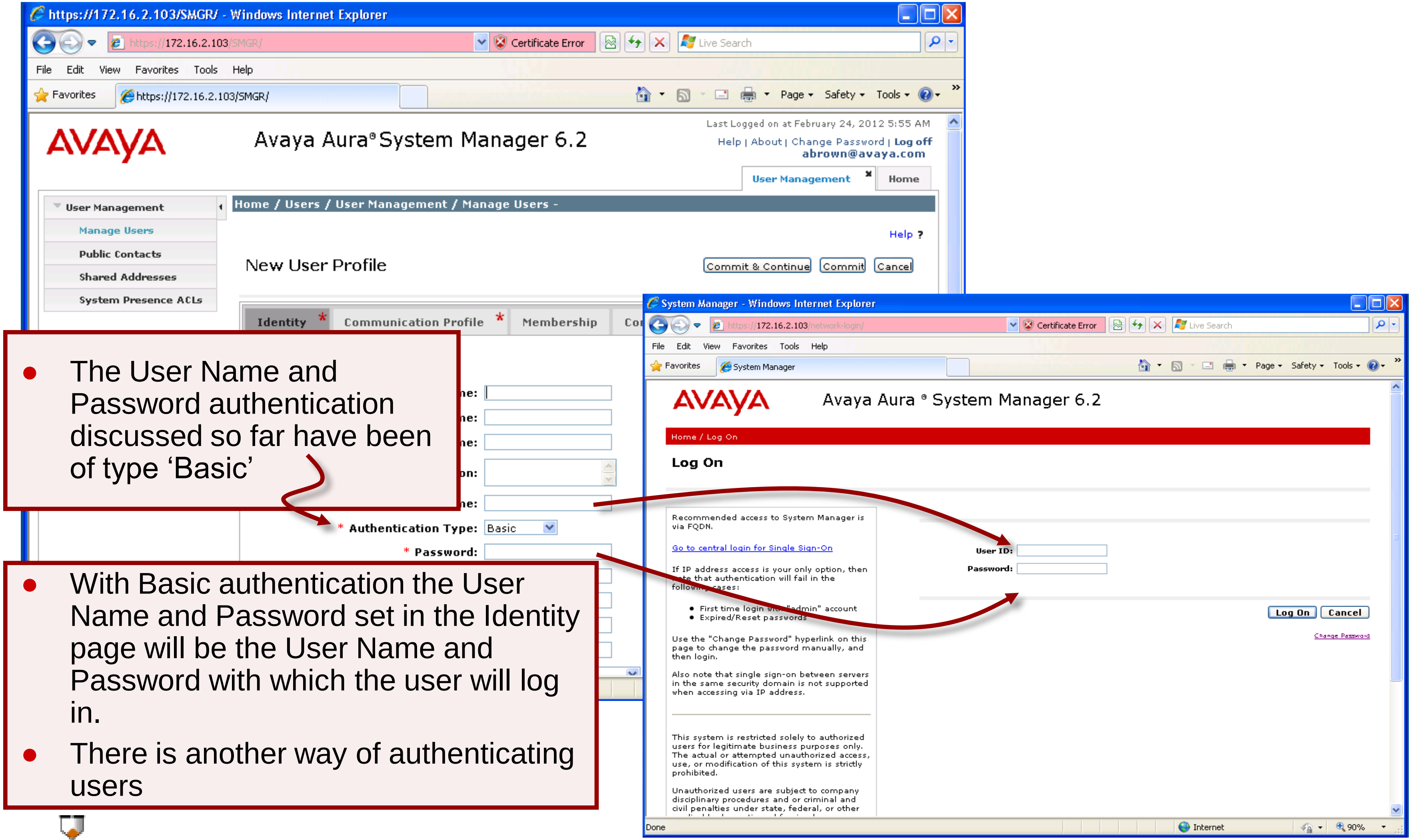
AVAYA | LEARNING

Module 03: System Manager User Administration

Lesson 02: User Authentication

Lesson Duration: 30 Minutes

Logon Authentication & LDAP



https://172.16.2.103/SMGR/ - Windows Internet Explorer
https://172.16.2.103/SMGR/
Certificate Error
Live Search
File Edit View Favorites Tools Help
Favorites
Page Safety Tools
AVAYA
Avaya Aura® System Manager 6.2
Last Logged on at February 24, 2012 5:55 AM
Help | About | Change Password | Log off
abrown@avaya.com
User Management
Home
User Management
Manage Users
Public Contacts
Shared Addresses
System Presence ACLs
Home / Users / User Management / Manage Users -
Help ?
New User Profile
Commit & Continue
Commit
Cancel
Identity *
Communication Profile *
Membership

- The User Name and Password authentication discussed so far have been of type 'Basic'

* Authentication Type: Basic

* Password:

- With Basic authentication the User Name and Password set in the Identity page will be the User Name and Password with which the user will log in.
- There is another way of authenticating users

System Manager - Windows Internet Explorer
https://172.16.2.103/network-login/
Certificate Error
Live Search
File Edit View Favorites Tools Help
Favorites
System Manager
Page Safety Tools
AVAYA
Avaya Aura ® System Manager 6.2
Home / Log On
Log On
User ID:
Password:
Log On
Cancel
Change Password
Done
Internet
90%

Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

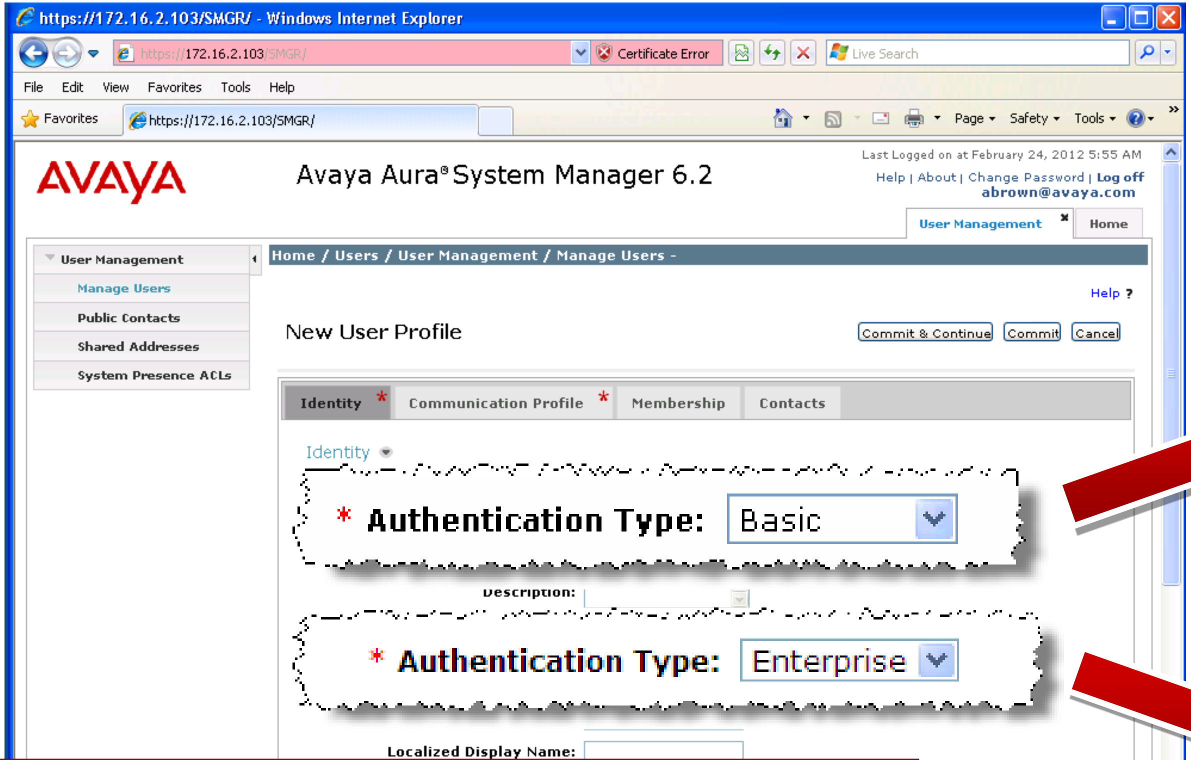
Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other

Lesson Duration: 30 Minutes

Topic 4: Logon Authentication & LDAP



https://172.16.2.103/SMGR/ - Windows Internet Explorer

https://172.16.2.103/SMGR/ Certificate Error Live Search

File Edit View Favorites Tools Help

Favorites https://172.16.2.103/SMGR/ Page Safety Tools

AVAYA Avaya Aura® System Manager 6.2

Last Logged on at February 24, 2012 5:55 AM

Help | About | Change Password | Log off

abrown@avaya.com

User Management Home

User Management

- Manage Users
- Public Contacts
- Shared Addresses
- System Presence ACLs

Home / Users / User Management / Manage Users -

Help ?

New User Profile

Commit & Continue Commit Cancel

Identity * Communication Profile * Membership Contacts

Identity

* Authentication Type: Basic

Description:

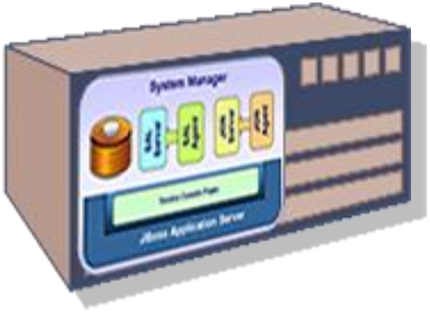
* Authentication Type: Enterprise

Localized Display Name:

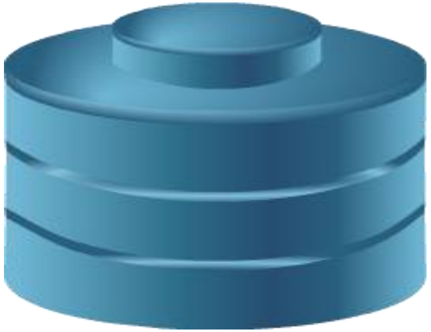
90%

- ‘Enterprise’ level authentication uses an LDAP (Lightweight directory access protocol) database such as Microsoft Active Directory, Lotus Domino, or Open LDAP.
- SMGR can synchronise users with that directory, and then subsequently to authenticate those users against that directory each time they log in

Local Authentication



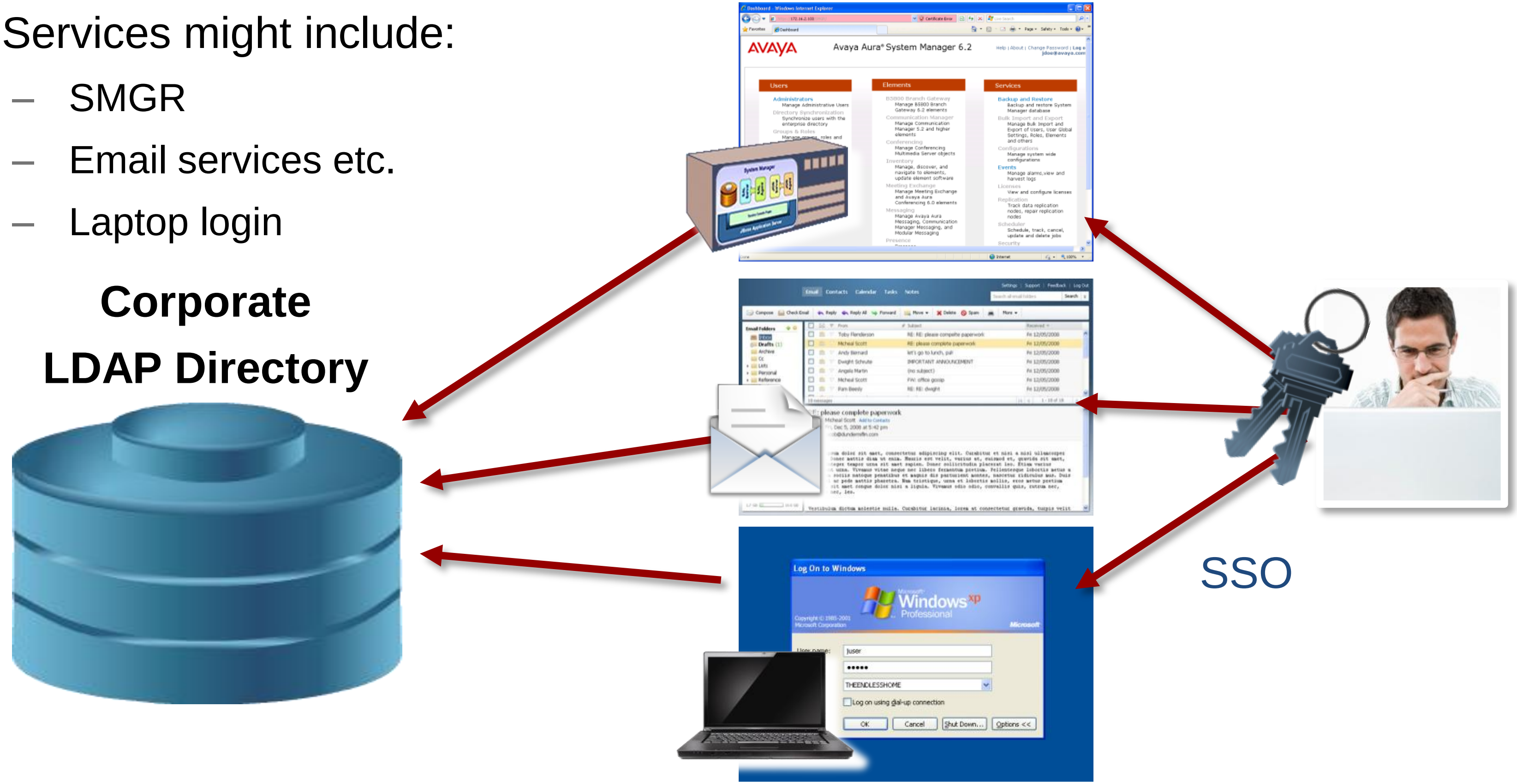
Corporate LDAP Directory



LDAP Integration

LDAP Server?

- SMGR can be configured to authenticate against a central LDAP server
- In this way, an enterprise can extend the use of a single sign-on (SSO) for *all* their core services – Aura & enterprise
- Services might include:
  - SMGR
  - Email services etc.
  - Laptop login



Corporate

LDAP Directory

SSO

Administrators
Manage Administrative Users
Directory Synchronization
Synchronize users with the enterprise directory
Groups & Roles
Manage groups, roles and

B5800 Branch Gateway
Manage B5800 Branch Gateway 6.2 elements
Communication Manager
Manage Communication Manager 5.2 and higher elements
Conferencing
Manage Conferencing Multimedia Server objects
Inventory
Manage, discover, and navigate to elements, update element software
Meeting Exchange
Manage Meeting Exchange and Avaya Aura Conferencing 6.0 elements
Messaging
Manage Avaya Aura Messaging, Communication Manager Messaging, and Modular Messaging
Presence

Backup and Restore
Backup and restore System Manager database
Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others
Configurations
Manage system wide configurations
Events
Manage alarms,view and harvest logs
Licenses
View and configure licenses
Replication
Track data replication nodes, repair replication nodes
Scheduler
Schedule, track, cancel, update and delete jobs
Security

Copyright © 1985-2001 Microsoft Corporation

User name: juser

Password: •••••

THEENDLESSHOME

□ Log on using dial-up connection

LDAP Integration (continued)

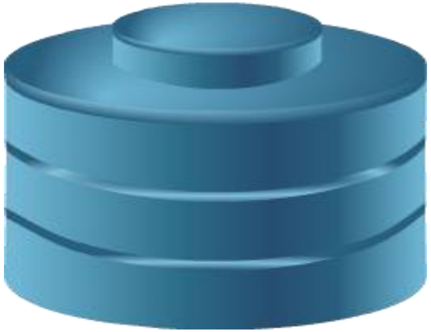
LDAP v. SMGR

What about SMGRs role as the central user database?

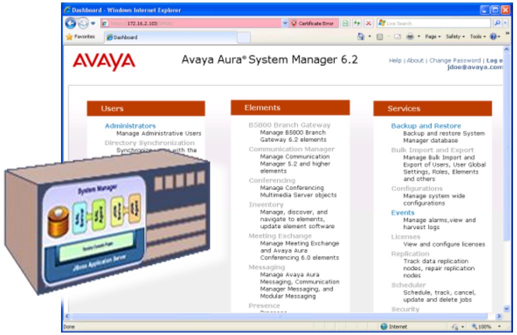
- SMGR is still the central place for Aura product admin
- Using LDAP to populate SMGR with users & authenticate them can be very convenient – especially for an enterprise with lots of users already in an LDAP server

Corporate

LDAP Directory



V.



AVAYA Avaya Aura® System Manager 6.2

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the

Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway 6.2 elements

Communication Manager
Manage Communication Manager 5.2 and higher elements

Conferencing
Manage Conferencing Multimedia Server objects

Inventory
Manage, discover, and navigate to elements, update element software

Meeting Exchange
Manage Meeting Exchange and Avaya Aura Conferencing 6.0 elements

Messaging
Manage Avaya Aura Messaging, Communication Manager Messaging, and Modular Messaging

Presence

Services

Backup and Restore
Backup and restore System Manager database

Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

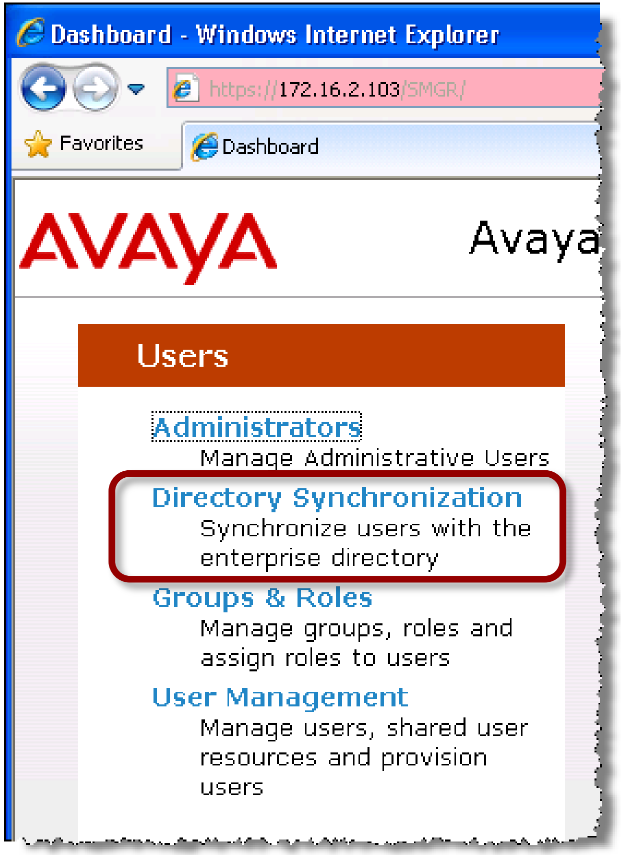
Replication
Track data replication nodes, repair replication nodes

Scheduler
Schedule, track, cancel, update and delete jobs

Security

LDAP Integration (continued)

- Synch SMGR with LDAP (Populate SMGR with users)



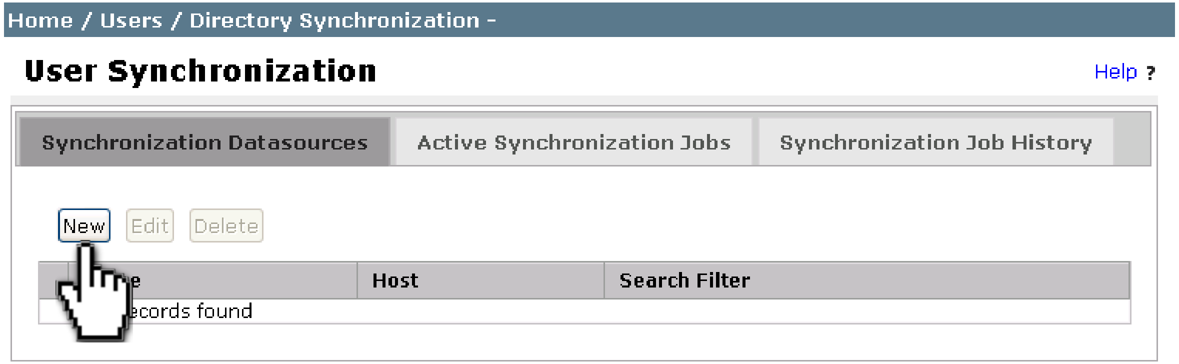
Dashboard - Windows Internet Explorer
https://172.16.2.103/SMGR/
Favorites
Dashboard
AVAYA
Avaya
Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

User Management
Manage users, shared user resources and provision users

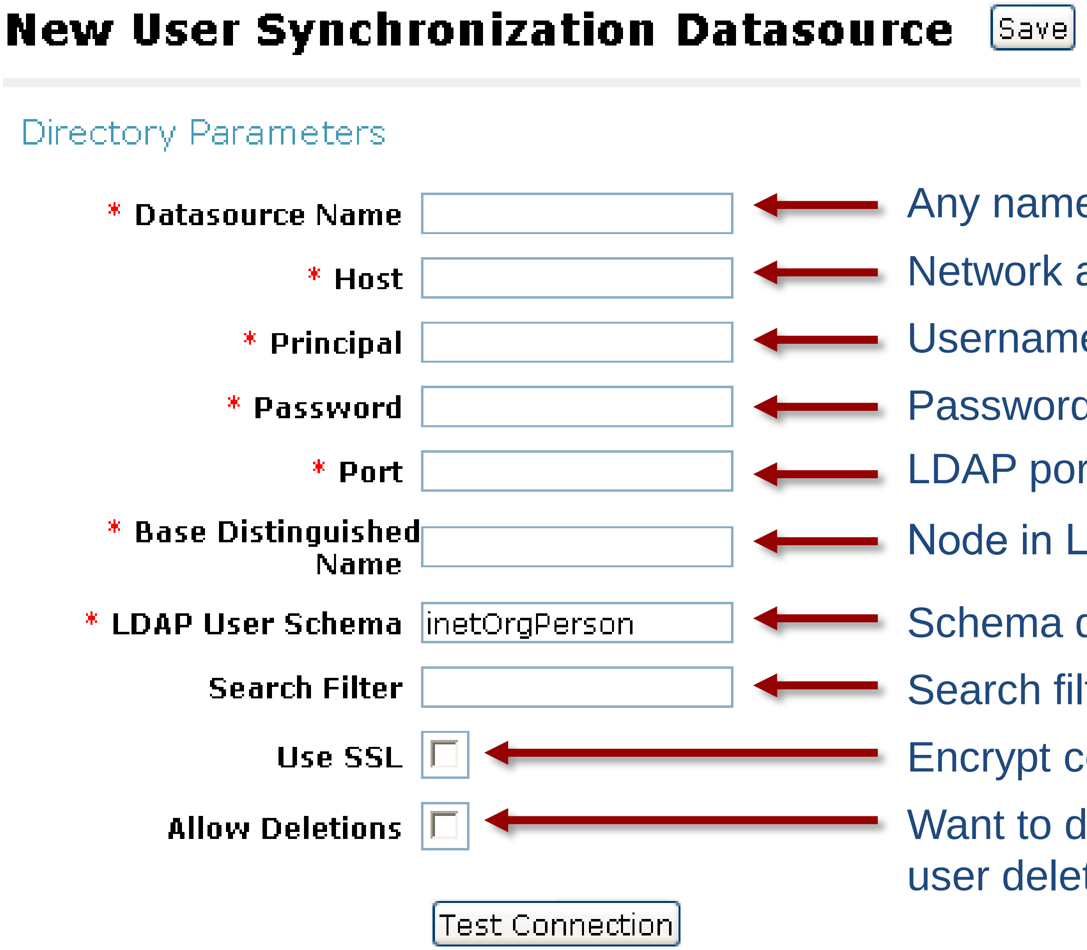


Home / Users / Directory Synchronization -
User Synchronization
Help ?
Synchronization Datasources
Active Synchronization Jobs
Synchronization Job History
New
Edit
Delete

...e	Host	Search Filter
...ecords found		

LDAP Integration (continued)

- Configure LDAP data source



New User Synchronization Datasource Save

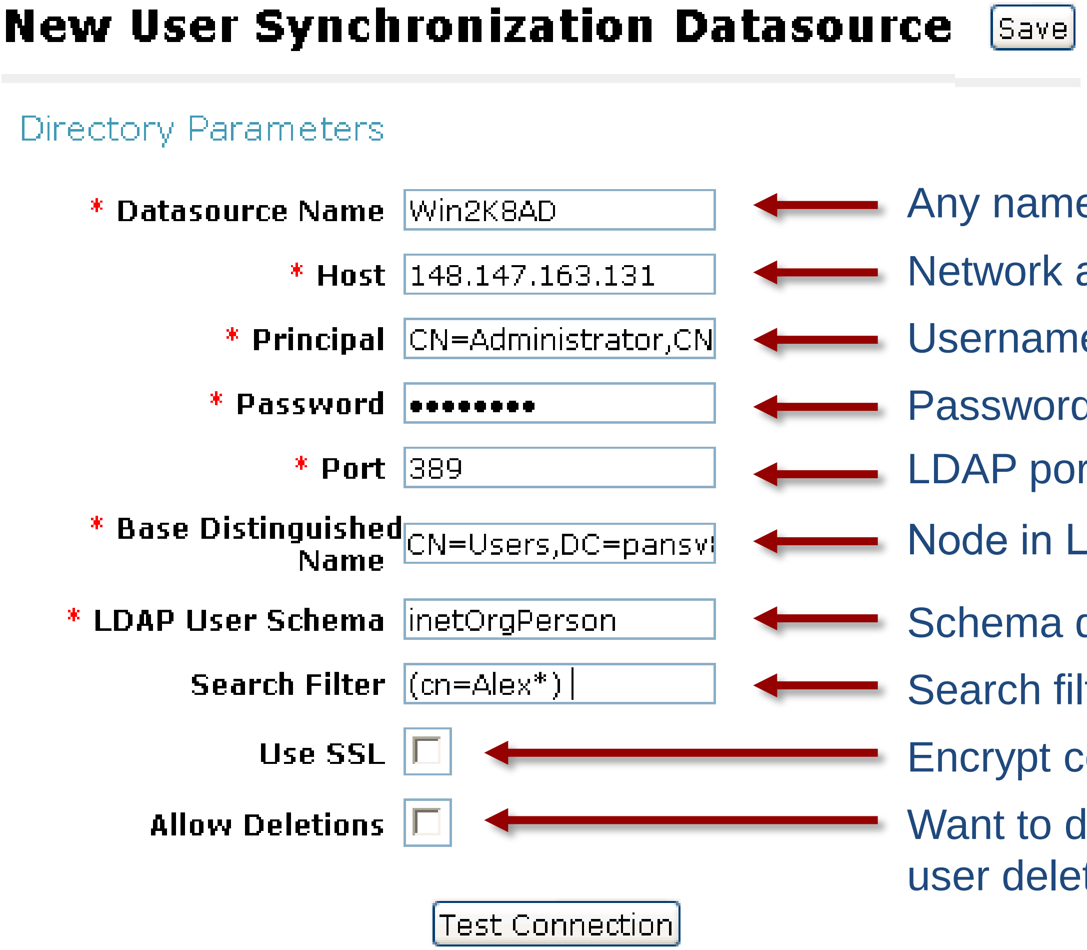
Directory Parameters

* Datasource Name		Any name you want
* Host		Network address of LDAP server
* Principal		Username with permission to create / update users
* Password		Password of principal LDAP user
* Port		LDAP port (default: 339)
* Base Distinguished Name		Node in LDAP tree where users will be sync'd from
* LDAP User Schema	inetOrgPerson	Schema defines object mappings
Search Filter		Search filter for matching entities
Use SSL	□	Encrypt connection to server
Allow Deletions	□	Want to delete an already synchronized user deleted from the Active Directory

Test Connection

LDAP Integration (continued)

- Configure LDAP data source



New User Synchronization Datasource

Directory Parameters

* Datasource Name	Win2K8AD	Any name you want
* Host	148.147.163.131	Network address of LDAP server
* Principal	CN=Administrator,CN	Username with permission to create / update users
* Password	●●●●●●●●●	Password of principal LDAP user
* Port	389	LDAP port (default: 339)
* Base Distinguished Name	CN=Users,DC=pansvi	Node in LDAP tree where users will be sync'd from
* LDAP User Schema	inetOrgPerson	Schema defines object mappings
Search Filter	(cn=Alex*)	Search filter for matching entities
Use SSL	□	Encrypt connection to server
Allow Deletions	□	Want to delete an already synchronized user deleted from the Active Directory

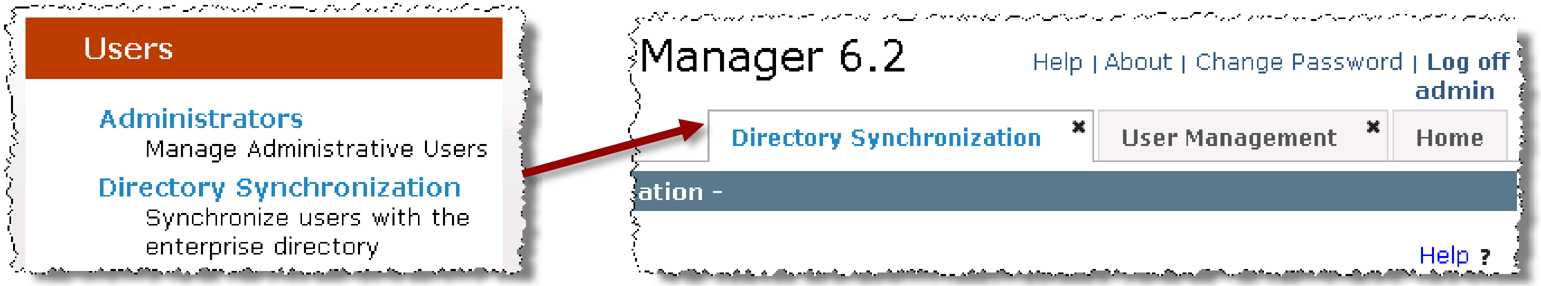
Exercise: Locate & Inspect LDAP Synchronization Screens

Objective & Outcome

Although there is no LDAP server running in the training lab, the objective of this exercise is to navigate to the LDAP screens and familiarise yourself with them.

1. Navigate to Users > Directory Synchronisation
2. Clicking '***New***' to create a dummy sync data source
3. Inspect the synch attribute fields. Be sure not to commit any changes.

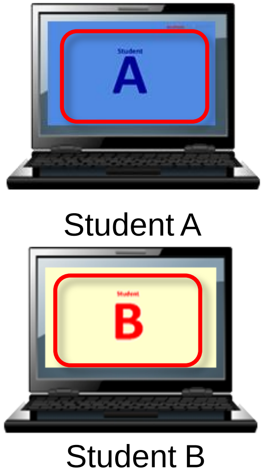
Individual Exercise – both students can work simultaneously



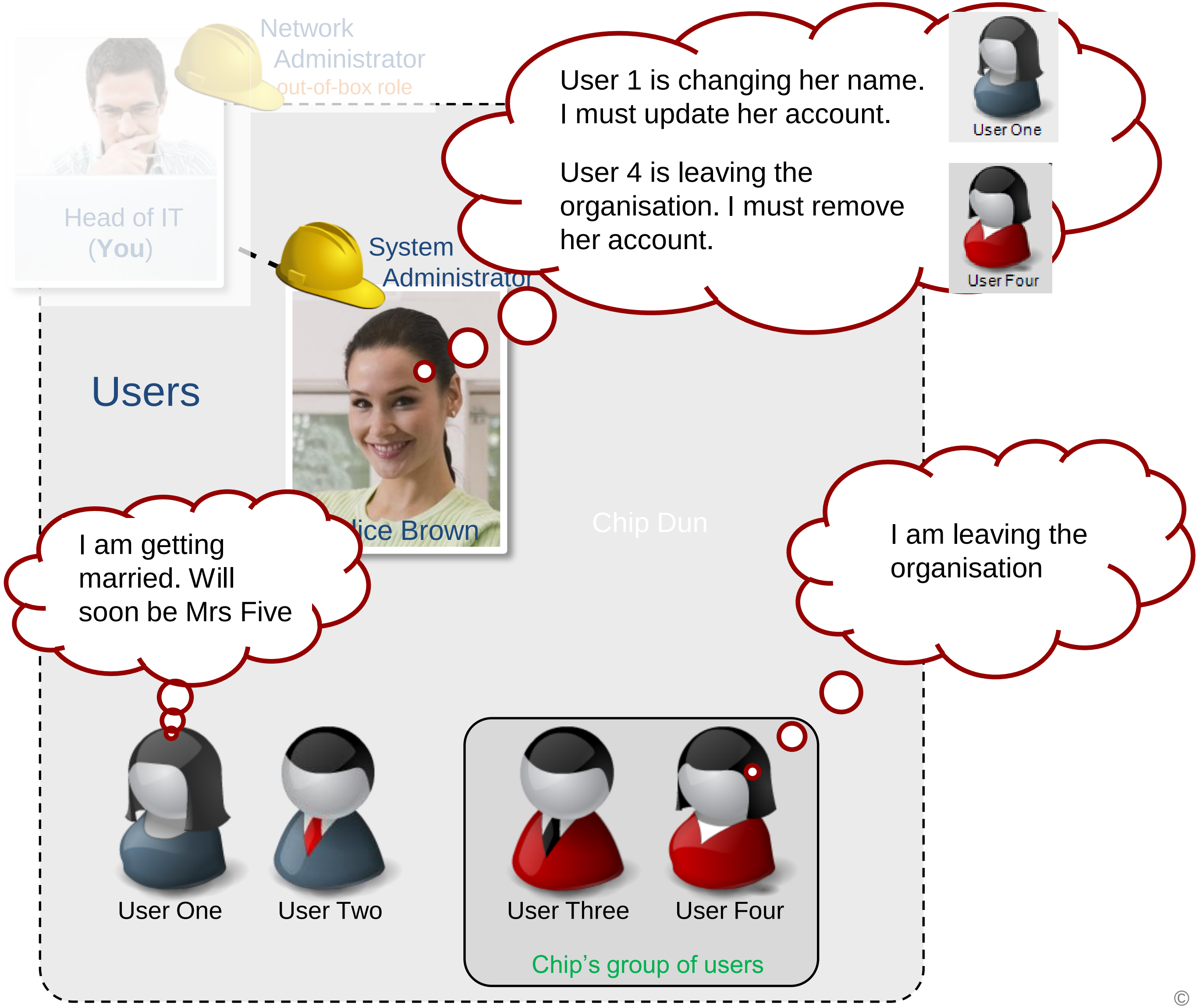
Users
Administrators
Directory Synchronization
Manager 6.2
Help | About | Change Password | Log off admin
Directory Synchronization
User Management
Home
ation -
Help ?

Manage Administrative Users

Synchronize users with the enterprise directory



Updating and Deleting a User



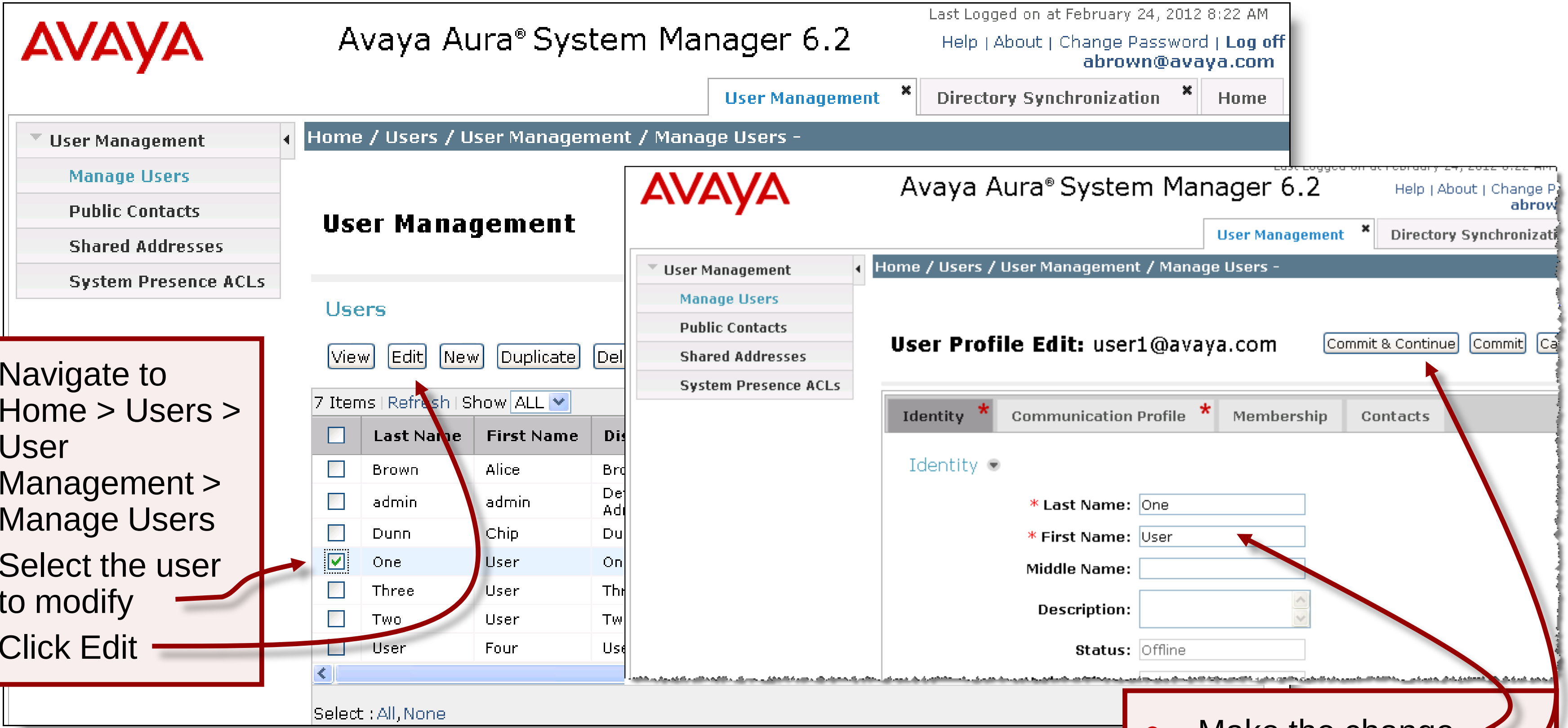
User 1 is changing her name. I must update her account.

User 4 is leaving the organisation. I must remove her account.

I am getting married. Will soon be Mrs Five

I am leaving the organisation

Updating Details in a User Profile



AVAYA Avaya Aura® System Manager 6.2

Last Logged on at February 24, 2012 8:22 AM

Help | About | Change Password | **Log off**
abrown@avaya.com

Home / Users / User Management / Manage Users -

User Management

Users

7 Items | Refresh | Show ALL

□	Last Name	First Name	Dis
□	Brown	Alice	Bro
□	admin	admin	De Adı
□	Dunn	Chip	Du
☑	One	User	On
□	Three	User	Thr
□	Two	User	Tw
□	User	Four	Use

Select : All, None

AVAYA Avaya Aura® System Manager 6.2

Help | About | Change P
abrow

Home / Users / User Management / Manage Users -

User Profile Edit: user1@avaya.com

Identity

* **Last Name:** One

* **First Name:** User

Middle Name:

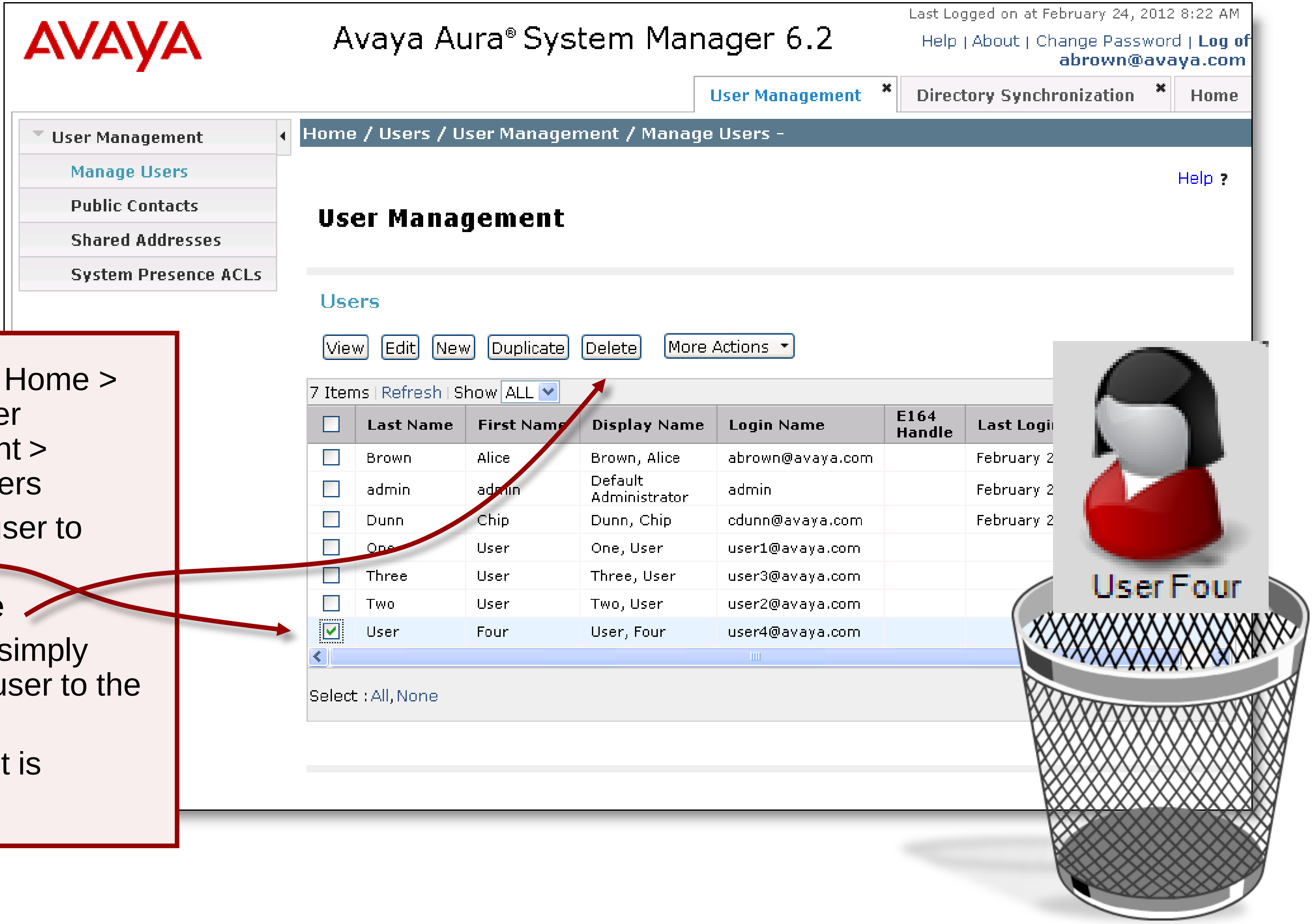
Description:

Status: Offline

- Navigate to Home > Users > User Management > Manage Users
- Select the user to modify
- Click Edit

- Make the change
- Click Commit

Deleting Users



Avaya Aura® System Manager 6.2
Last Logged on at February 24, 2012 8:22 AM
Help | About | Change Password | Log of

Directory Synchronization

Home / Users / User Management / Manage Users -

User Management

Users

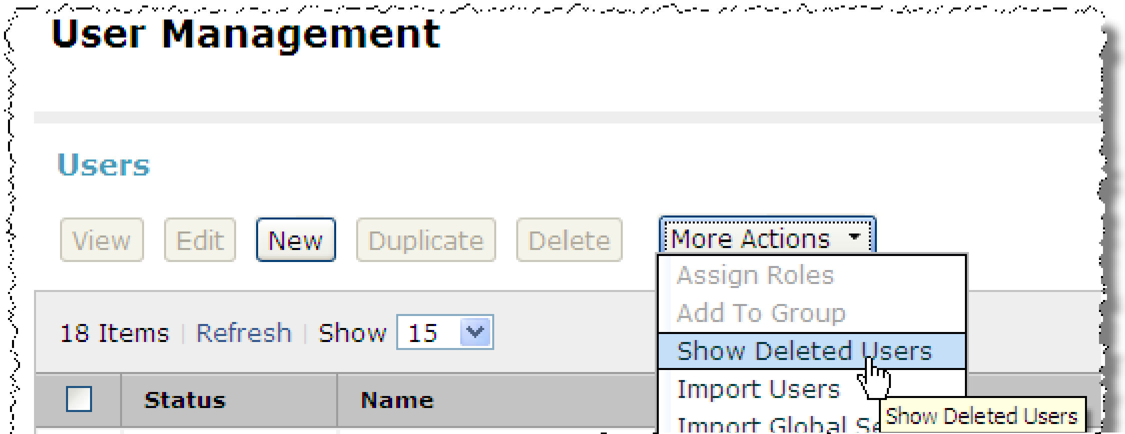
7 Items | Refresh | Show ALL

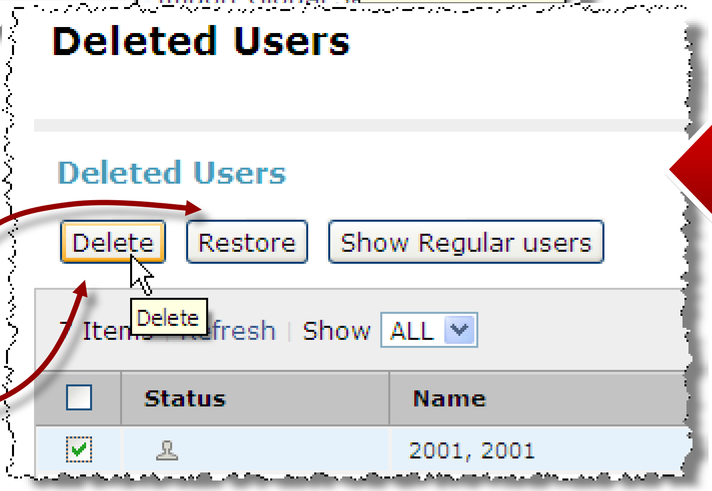
□	Last Name	First Name	Display Name	Login Name	E164 Handle	Last Logi
□	Brown	Alice	Brown, Alice	abrown@avaya.com		February 2
□	admin	admin	Default Administrator	admin		February 2
□	Dunn	Chip	Dunn, Chip	cdunn@avaya.com		February 2
□	One	User	One, User	user1@avaya.com		
□	Three	User	Three, User	user3@avaya.com		
□	Two	User	Two, User	user2@avaya.com		
☑	User	Four	User, Four	user4@avaya.com		

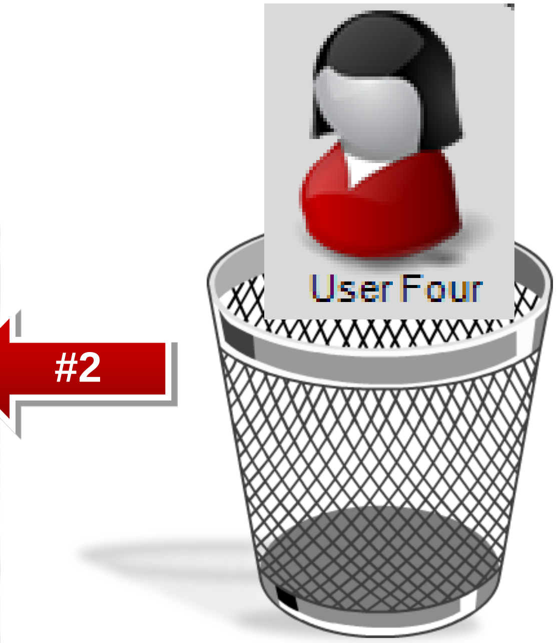
Select : All, None

- Navigate to Home > Users > User Management > Manage Users
- Select the user to delete
- Click Delete
- This action simply moves the user to the recycle bin.
- The account is suspended

Further Actions with Deleted Users: Restore/Delete







- SMGR keeps deleted users in the ‘recycle bin’
- Deleted users can be
  - Reinstated
  - Permanently deleted

  …through the More Actions menu

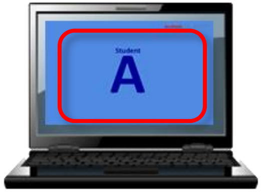
Exercise: Modifying and Deleting Users

Objective & Outcome

The objective of this exercise is to become familiar with the process of updating and deleting user profile accounts. By the time you are done, you will have changed a user's Last Name, deleted and reinstated one user and permanently deleted another.

1. **Change User One's Last Name** to Five
   - Navigate to Home > Users > User Management > Manage Users
   - Select User One. Click ***Edit***
   - Change the Last Name to 'Five'. Click ***Commit***
2. **Delete** User Two and User Four
   - Select User Two and User Four. Click ***Delete***. Confirm User Delete
   - Check the users no longer appear in the list of User Management users
3. **Reinstate** User Two
   - Click ***More Actions*** and select ***Show Deleted Users***
   - Select User Two and click ***Restore***
   - Confirm User Two should be restored.
   - Check that he is listed again with other users
4. **Permanently delete** User Four
   - Click ***More Actions*** and select ***Show Deleted Users***
   - Select User Four and click ***Delete***. Confirm User Four should be deleted.
   - Check that he is not listed with the other users

Individual Exercise – both students can work simultaneously



Student A

Student B

AVAYA | LEARNING

Module 04

Product Administration

Module Duration: 3 Hours

Module Objectives

After completing this module, you will:

- Have a feel for product administration.
  - Individual adopting product training is beyond the scope of this course.
  - Each adopting product will have its own specific training course.
- Be able to use SMGR to discover Avaya services in the network.
- Be able to use SMGR event & alarm logging features.
- Be able to configure SMGR to harvest logs.

Module Duration: 3 Hours

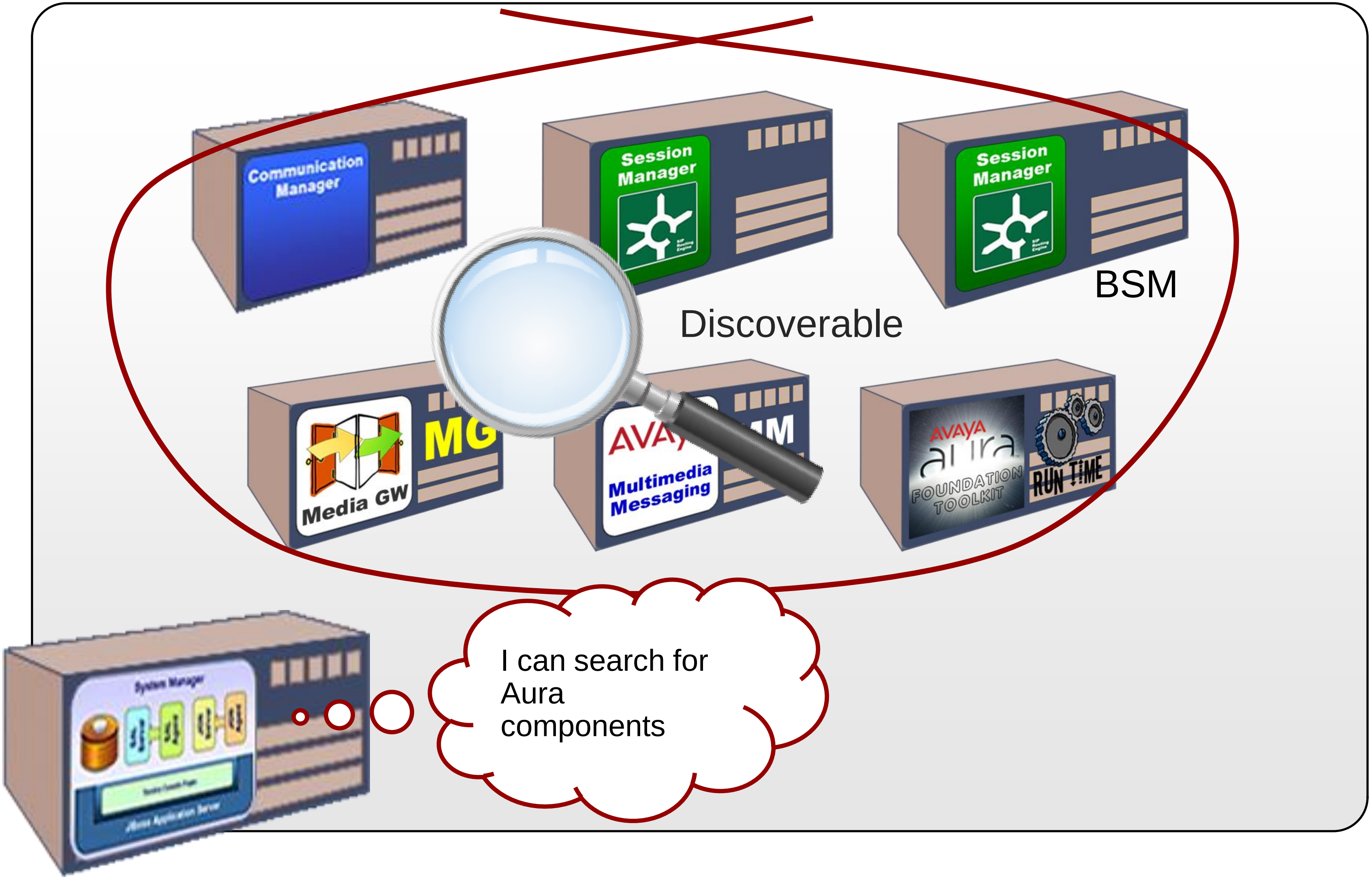
Module 04: Product Administration

Lesson 01: Inventory Discovery

Lesson Duration: 40 Minutes

Lesson Duration: 40 Minutes

Inventory Discovery



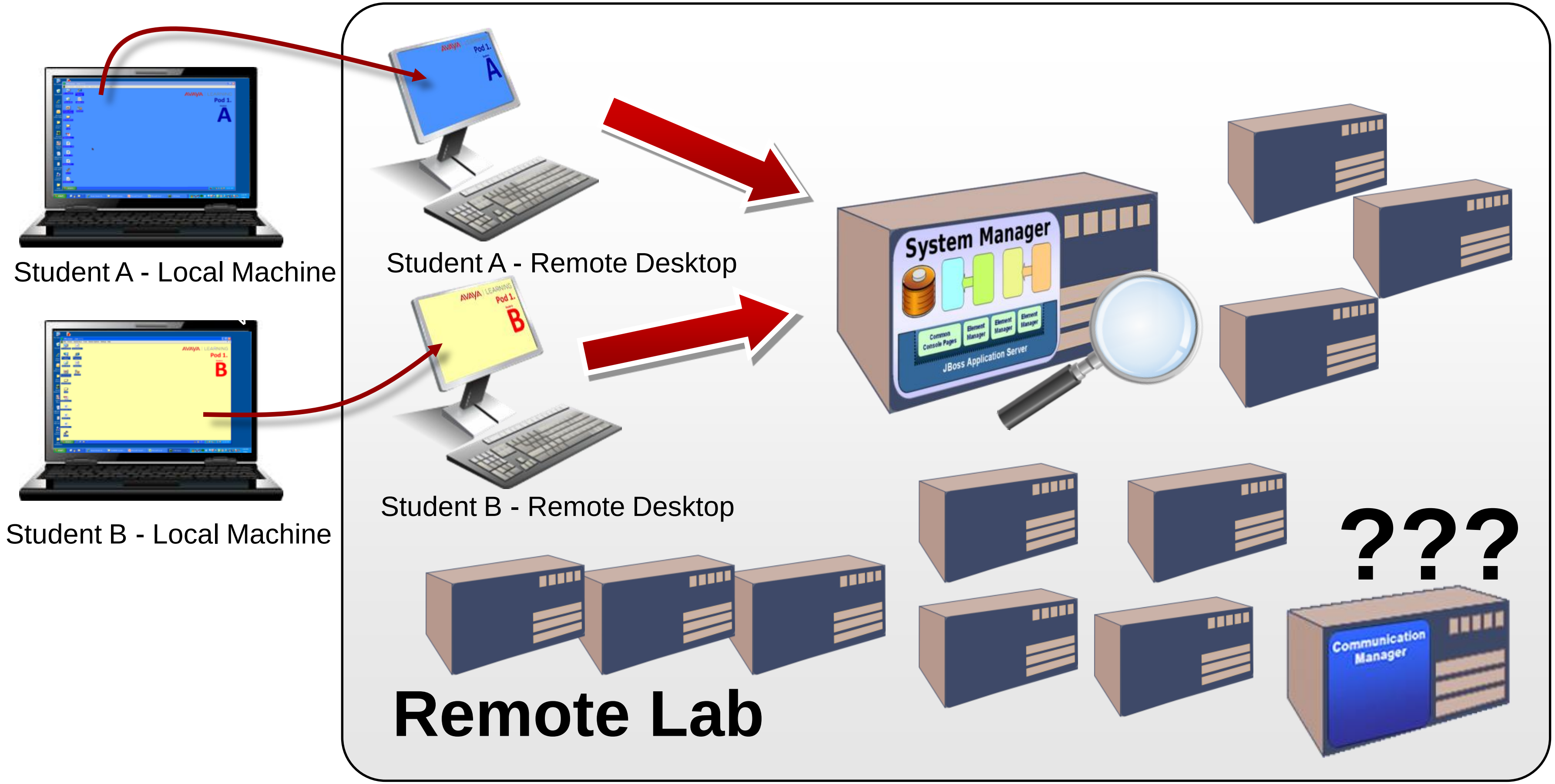
BSM

Discoverable

I can search for Aura components

SMGR Virtual Lab – Contains a CM

Next task: learn how to discover the CM in the remote lab.

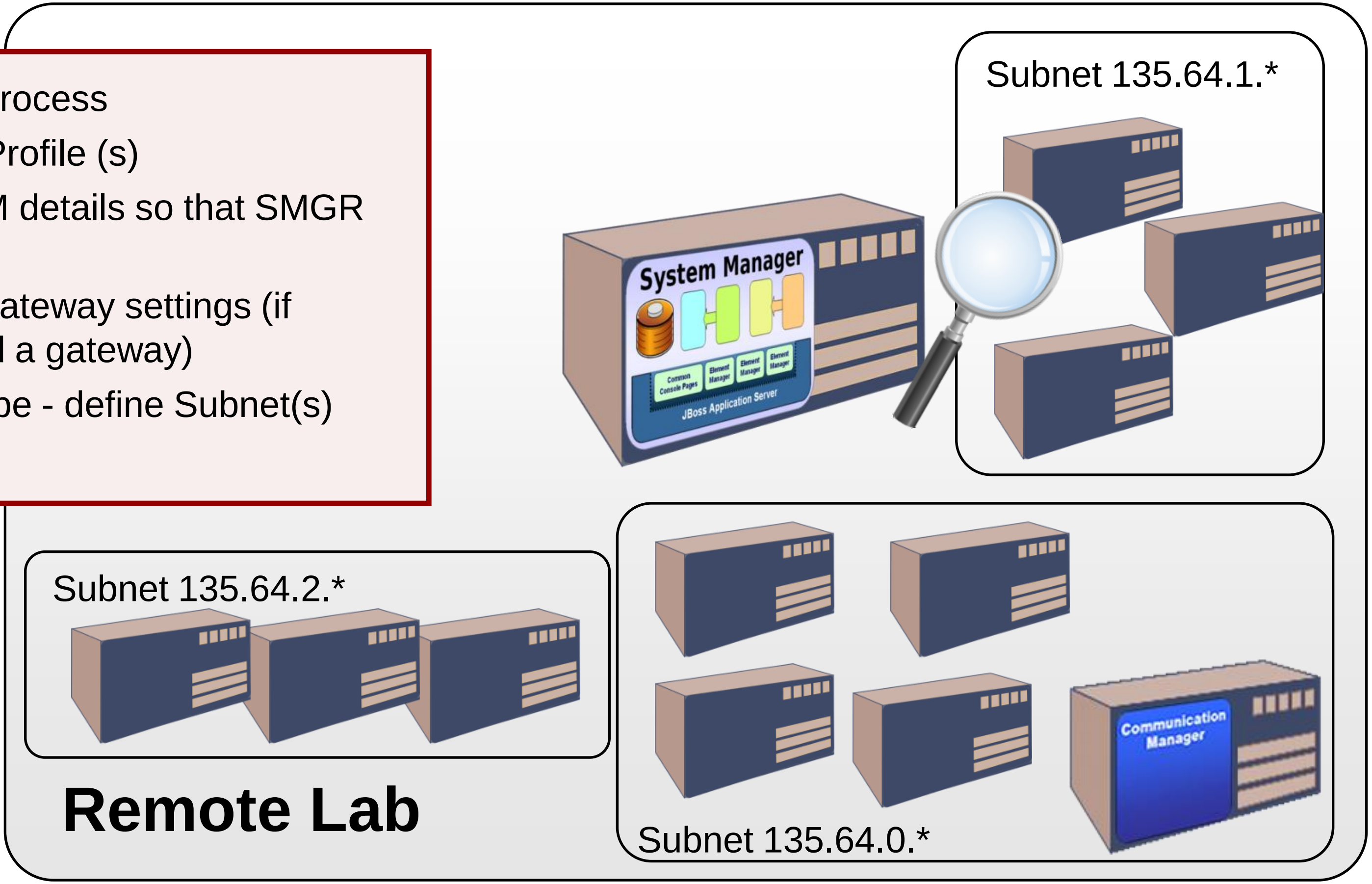


Inventory Discovery

Next task: learn how to discover the CM in the remote lab.

Discovery – a 5 step process

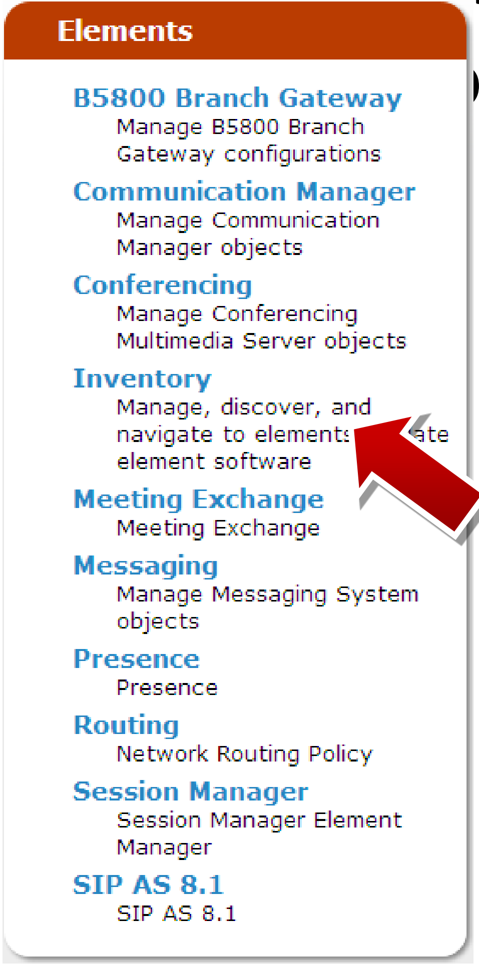
1. Configure SNMP Profile (s)
2. Optional: Enter CM details so that SMGR can auto synch
3. Optional: Define Gateway settings (if devices are behind a gateway)
4. Refine search scope - define Subnet(s)
5. Start discovery



(Check SNMP service is running on CM)

Inventory Discovery (continued)

- Navigate to Inventory > Discovery Management >



Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway configurations

Communication Manager
Manage Communication Manager objects

Conferencing
Manage Conferencing Multimedia Server objects

Inventory
Manage, discover, and navigate to element ate element software

Meeting Exchange
Meeting Exchange

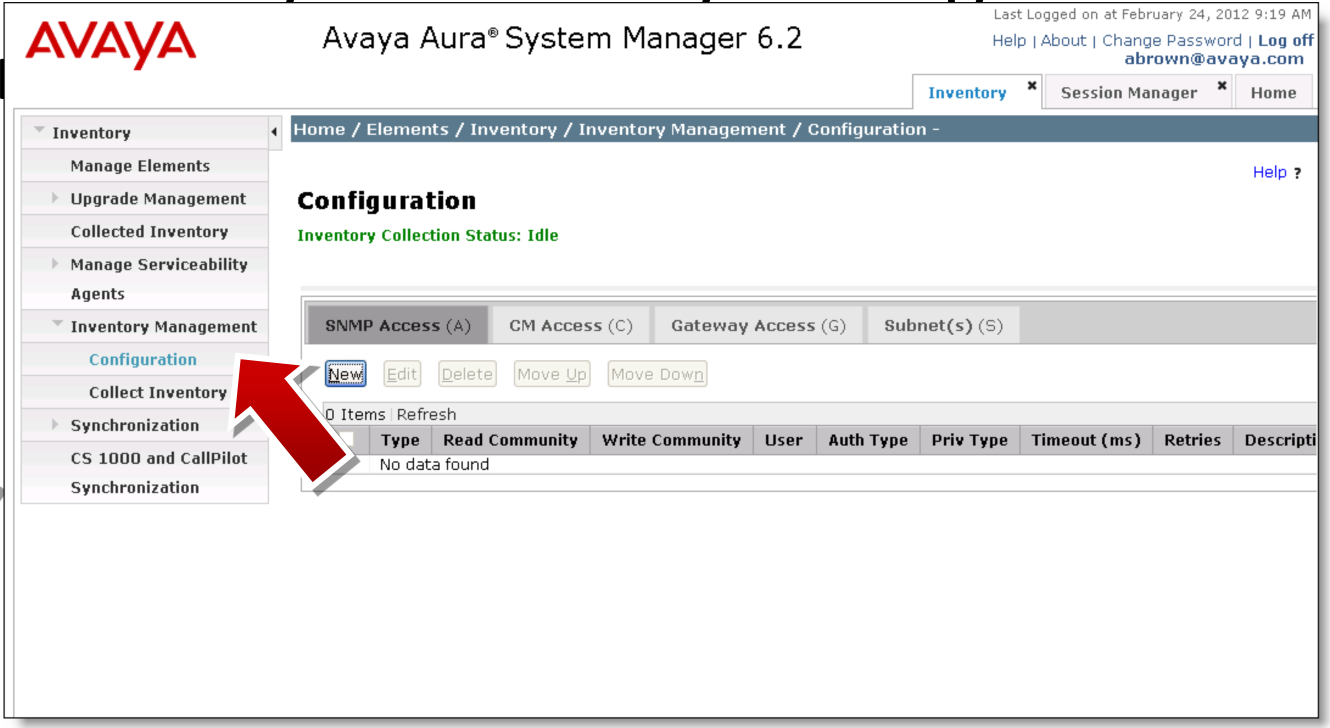
Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1



AVAYA Avaya Aura® System Manager 6.2

Last Logged on at February 24, 2012 9:19 AM
Help | About | Change Password | Log off abrown@avaya.com

Inventory | Session Manager | Home

Home / Elements / Inventory / Inventory Management / Configuration -

Configuration

Inventory Collection Status: Idle

0 Items | Refresh

	Type	Read Community	Write Community	User	Auth Type	Priv Type	Timeout (ms)	Retries	Descripti
	No data found								

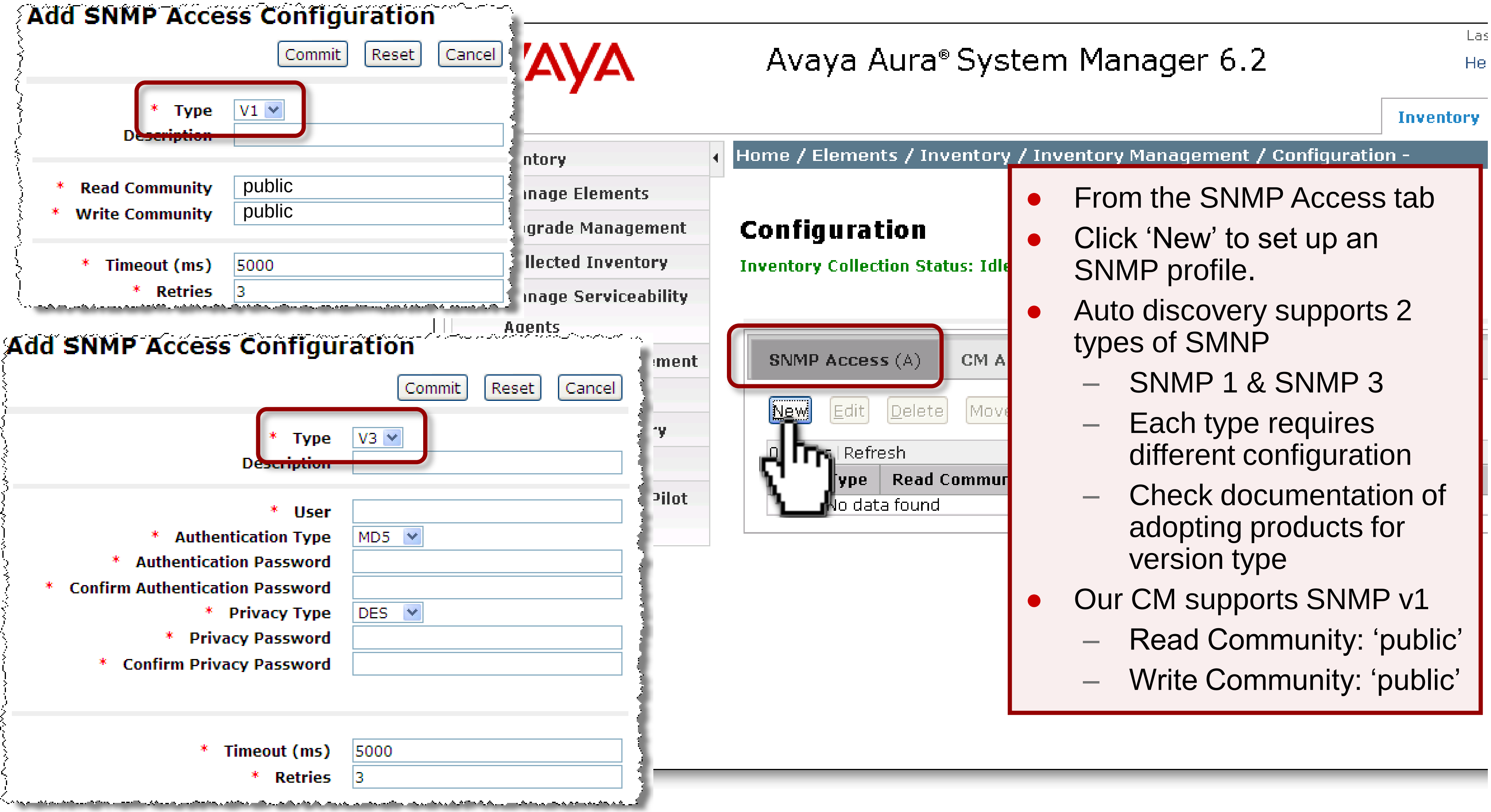
- Navigate to Home > Elements > Inventory > Inventory Management > Configuration

Note the 4 tabs:

- SMNP Access, SM Access, Gateway Access & Subnets

Inventory Discovery Step 1: Configuring SNMP

2 SNMP types



Add SNMP Access Configuration

* Type	V1
Description	
* Read Community	public
* Write Community	public
* Timeout (ms)	5000
* Retries	3

Add SNMP Access Configuration

* Type	V3
Description	
* User	
* Authentication Type	MD5
* Authentication Password	
* Confirm Authentication Password	
* Privacy Type	DES
* Privacy Password	
* Confirm Privacy Password	
* Timeout (ms)	5000
* Retries	3

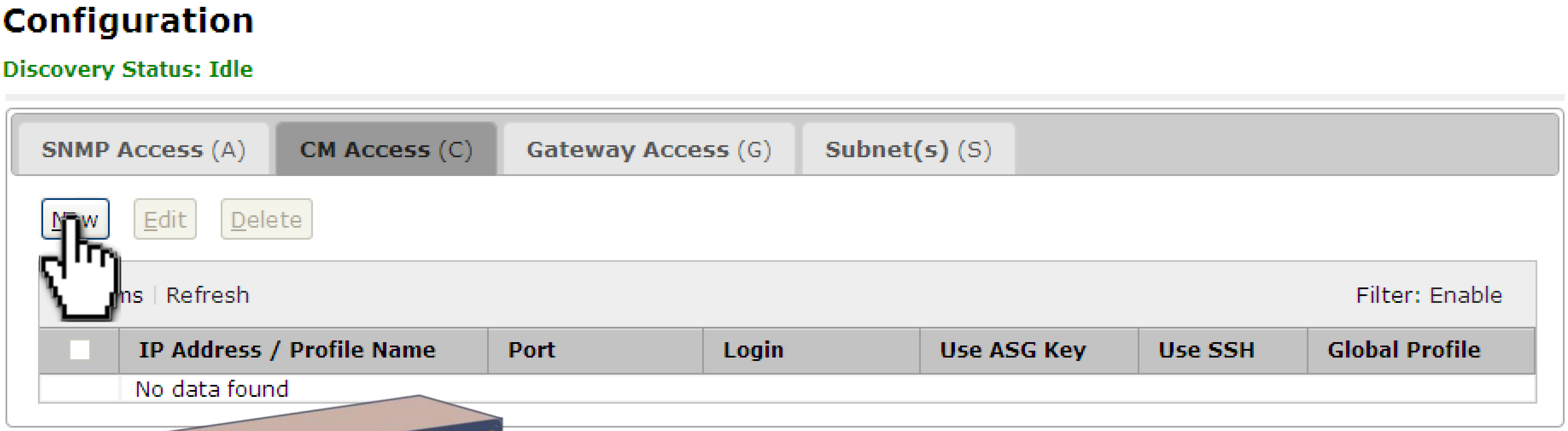
Configuration

Inventory Collection Status: Idle

No data found

- From the SNMP Access tab
- Click 'New' to set up an SNMP profile.
- Auto discovery supports 2 types of SMNP
  - SNMP 1 & SNMP 3
  - Each type requires different configuration
  - Check documentation of adopting products for version type
- Our CM supports SNMP v1
  - Read Community: 'public'
  - Write Community: 'public'

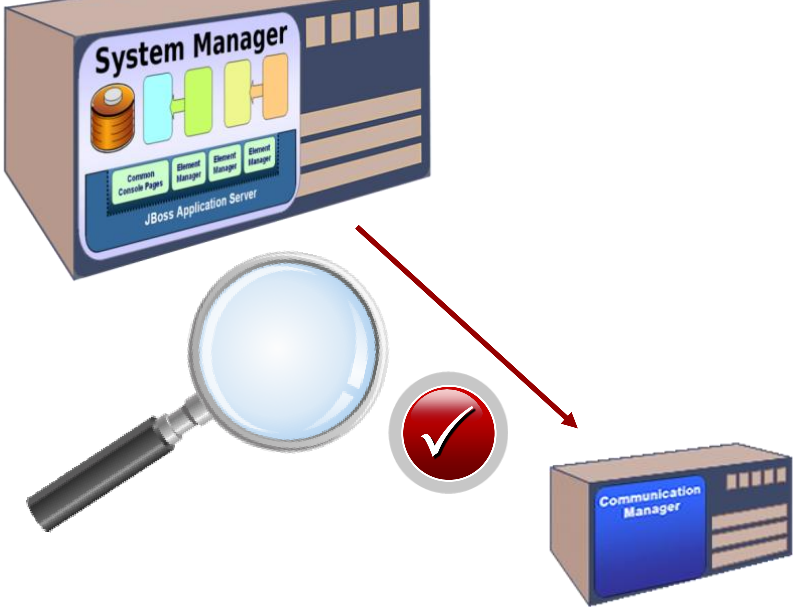
Inventory Discovery Step 2: Optional CM Access Config



Configuration

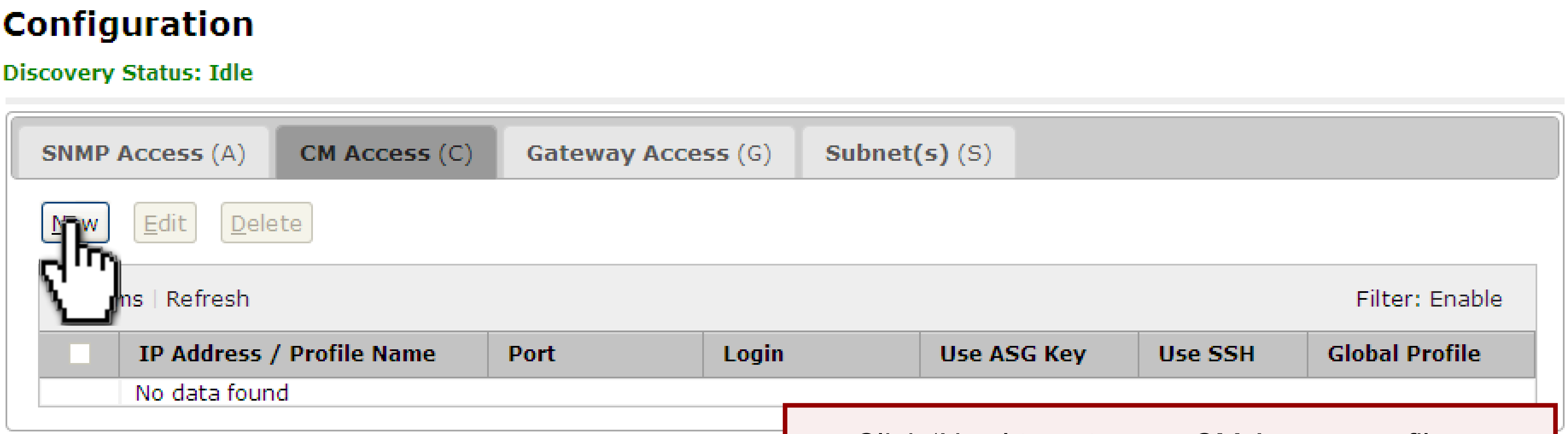
Discovery Status: Idle

□	IP Address / Profile Name	Port	Login	Use ASG Key	Use SSH	Global Profile
	No data found					



- A CM Access profile is optional.
- SMGR will still discover CM instances **without** a CM Access profile
- If a CM Access profile exists, it is used after discovery when SMGR attempts to automatically add and configure the discovered CMs

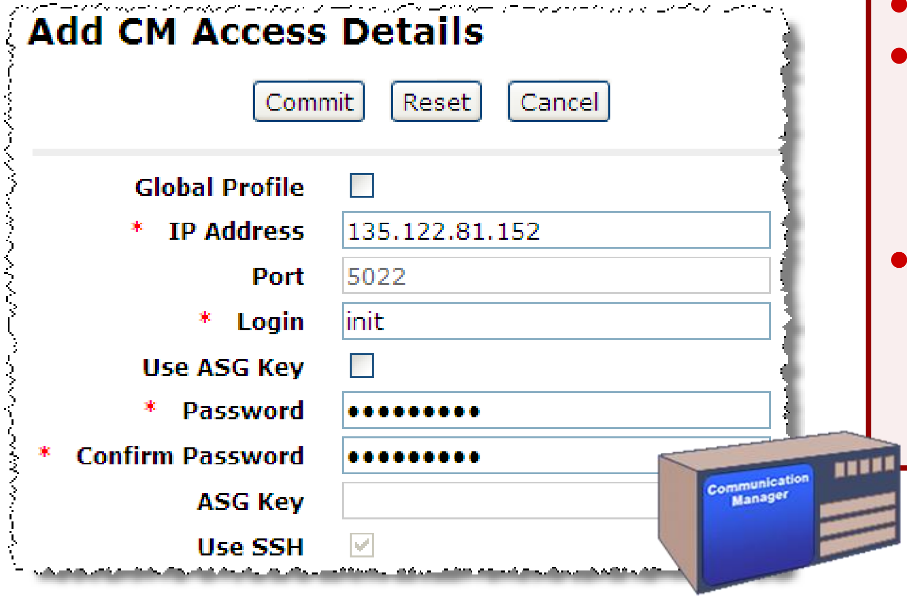
Inventory Discovery Step 2: Optional CM Access Config



Configuration

Discovery Status: Idle

☐	IP Address / Profile Name	Port	Login	Use ASG Key	Use SSH	Global Profile
	No data found					

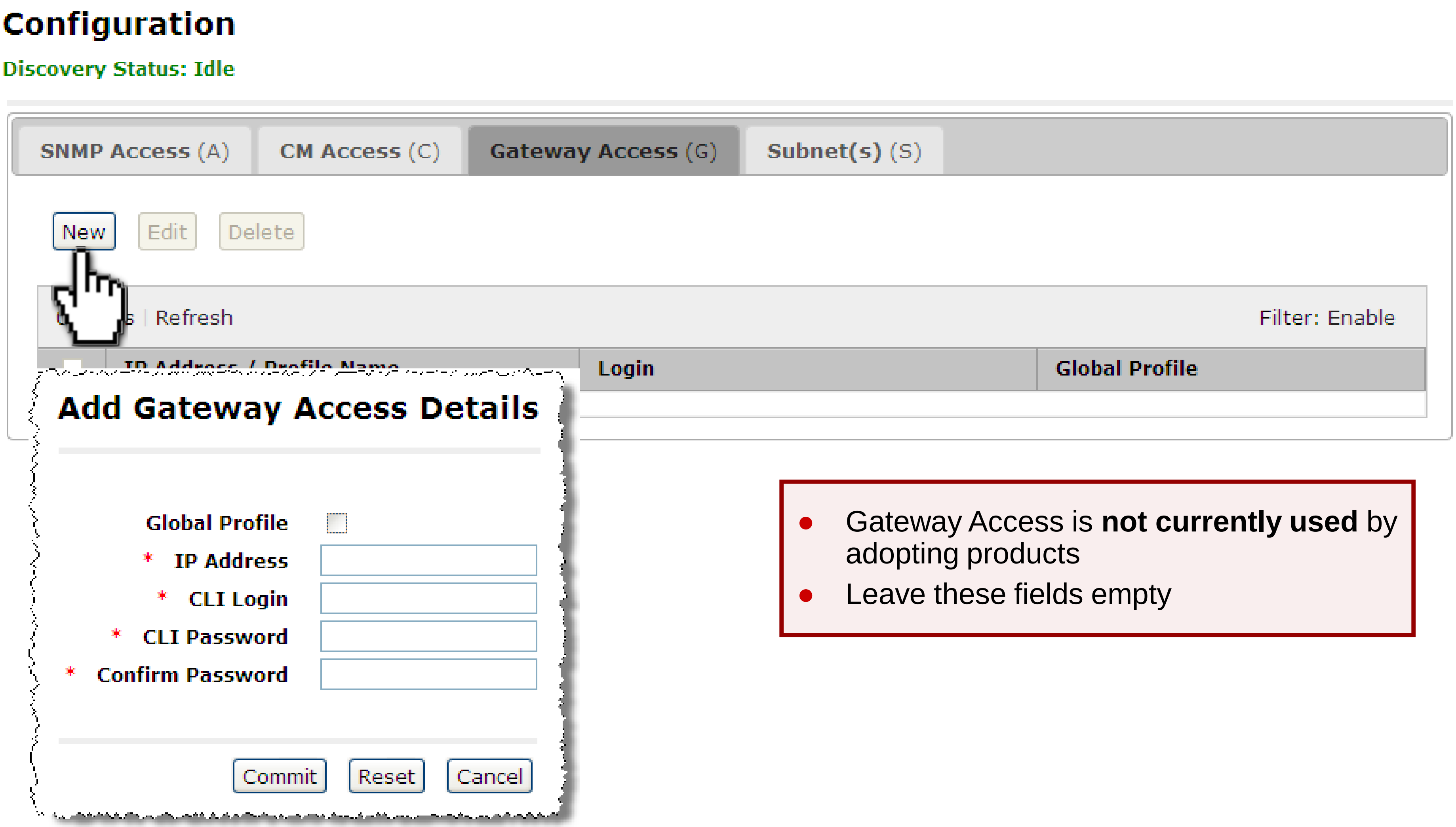


Add CM Access Details

Global Profile	☐
* IP Address	135.122.81.152
Port	5022
* Login	init
Use ASG Key	☐
* Password	●●●●●●●●●
* Confirm Password	●●●●●●●●●
ASG Key	
Use SSH	☑

- Click ‘New’ to set up an CM Access profile
- Required settings
  - CM IP address (!)
  - CM login: eg ‘craft’
  - CM password: eg ‘crftpw’
- If SMGR finds a CM it will compare the discovered IP with the IP’s we add to CM profiles. Finding a match it will then use the related username and password to add / synch the discovered CM

Inventory Discovery Step 3: Configuring Gateway Access



Configuration

Discovery Status: Idle

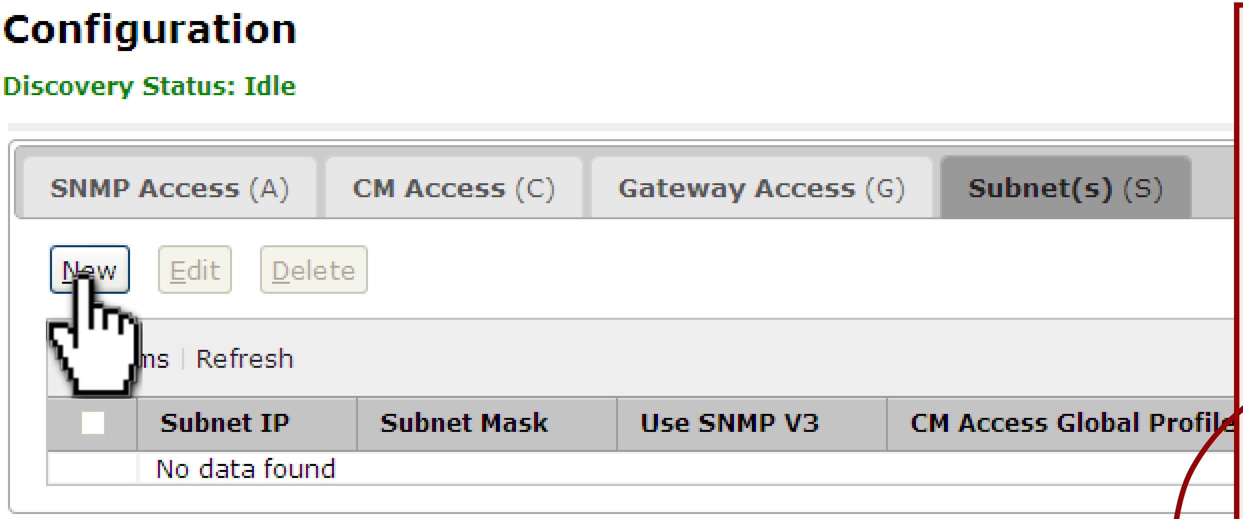
IP Address / Profile Name	Login	Global Profile

Add Gateway Access Details

Global Profile	□
* IP Address	
* CLI Login	
* CLI Password	
* Confirm Password	

- Gateway Access is **not currently used** by adopting products
- Leave these fields empty

Inventory Discovery Step 4: Refining Search with Subnets



Configuration

Discovery Status: Idle

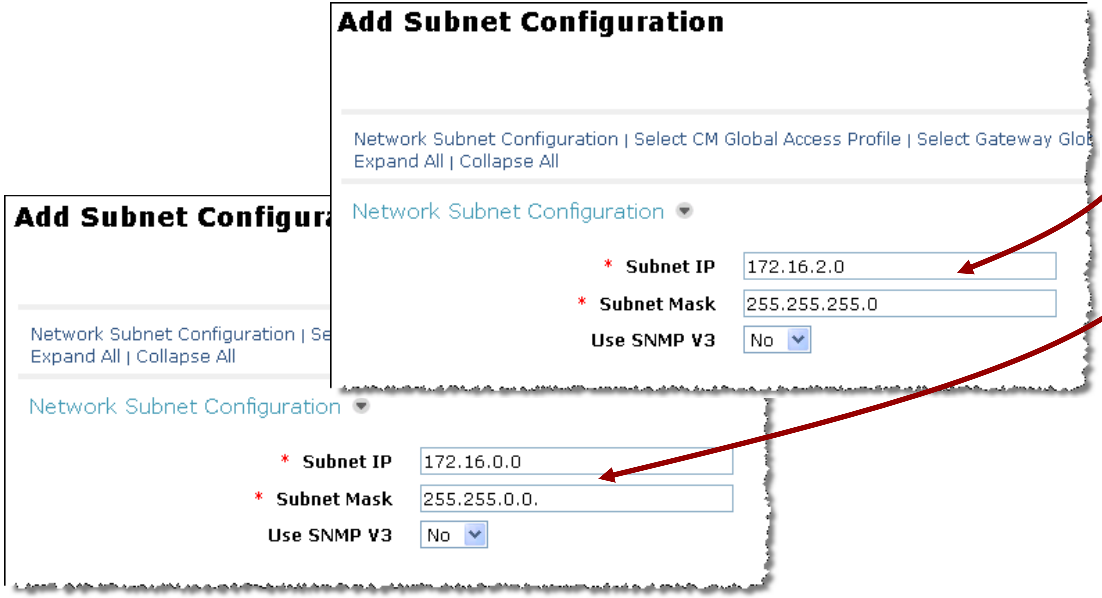
SNMP Access (A) | CM Access (C) | Gateway Access (G) | **Subnet(s) (S)**

New | Edit | Delete

ms | Refresh

□	Subnet IP	Subnet Mask	Use SNMP V3	CM Access Global Profile
	No data found			

- Click ‘New’ to set up a Subnet profile
- Required settings
  - Subnet IP pattern
  - Subnet mask
  - With a mask of 255.255.255.0 the IP’s final octet 0 is a wildcard – smaller search
  - With a mask of 255.255.0.0 the IP’s final two octets are wildcards – much bigger search



Add Subnet Configuration

Network Subnet Configuration | Select CM Global Access Profile | Select Gateway Glot
Expand All | Collapse All

Network Subnet Configuration

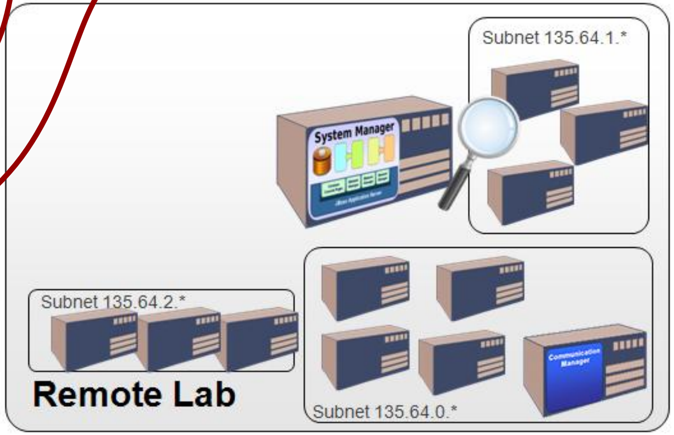
* Subnet IP	172.16.2.0
* Subnet Mask	255.255.255.0
Use SNMP V3	No

Add Subnet Configura

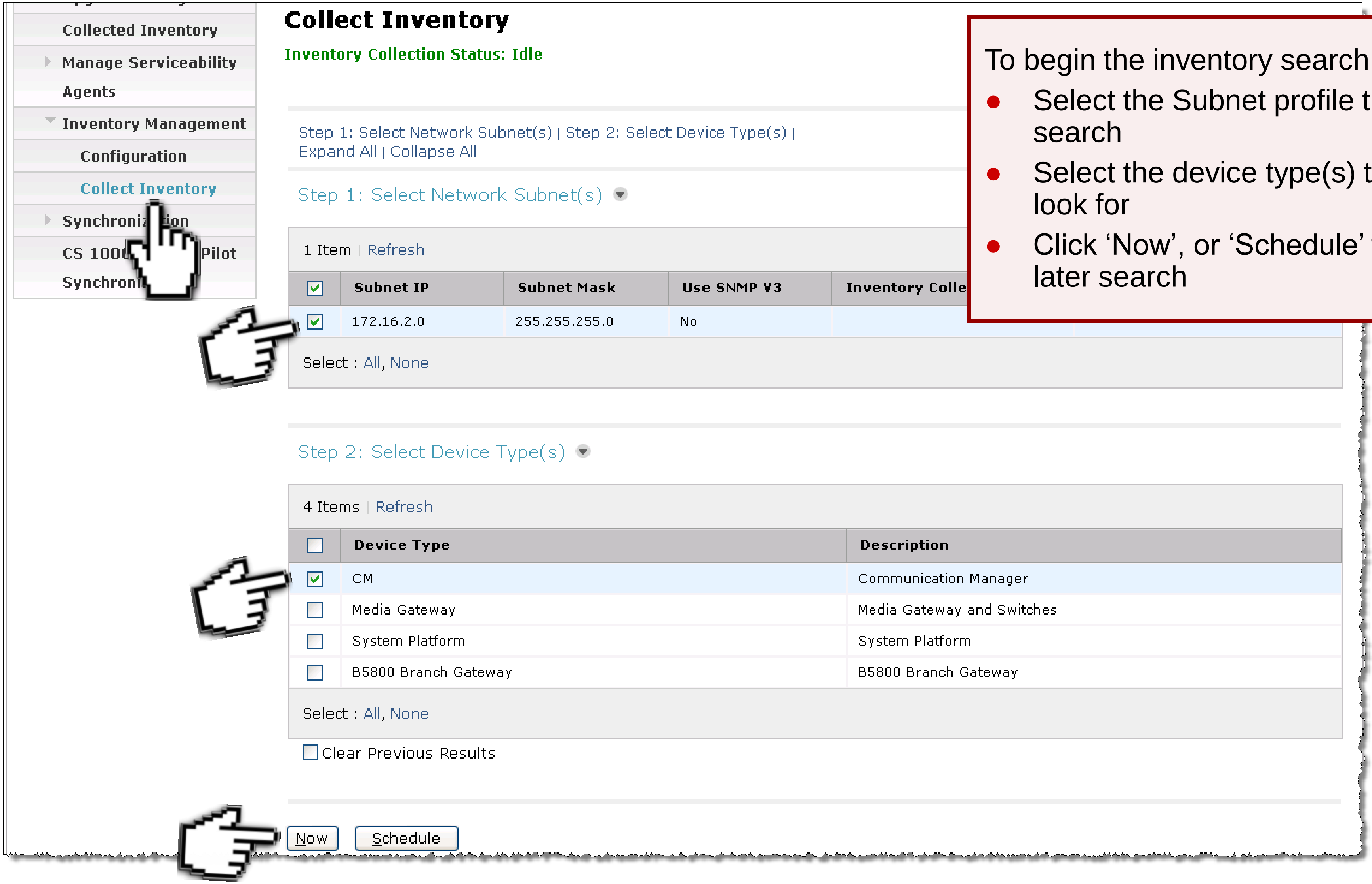
Network Subnet Configuration | Se
Expand All | Collapse All

Network Subnet Configuration

* Subnet IP	172.16.0.0
* Subnet Mask	255.255.0.0.
Use SNMP V3	No



Starting the Inventory Search



Collected Inventory

Manage Serviceability Agents

Inventory Management

Configuration

Collect Inventory

Synchronization

CS 1000 Pilot

Synchroni

Collect Inventory

Inventory Collection Status: Idle

Step 1: Select Network Subnet(s) | Step 2: Select Device Type(s) | Expand All | Collapse All

Step 1: Select Network Subnet(s)

1 Item | Refresh

☑	Subnet IP	Subnet Mask	Use SNMP V3	Inventory Colle
☑	172.16.2.0	255.255.255.0	No	

Select : All, None

Step 2: Select Device Type(s)

4 Items | Refresh

□	Device Type	Description
☑	CM	Communication Manager
□	Media Gateway	Media Gateway and Switches
□	System Platform	System Platform
□	B5800 Branch Gateway	B5800 Branch Gateway

Select : All, None

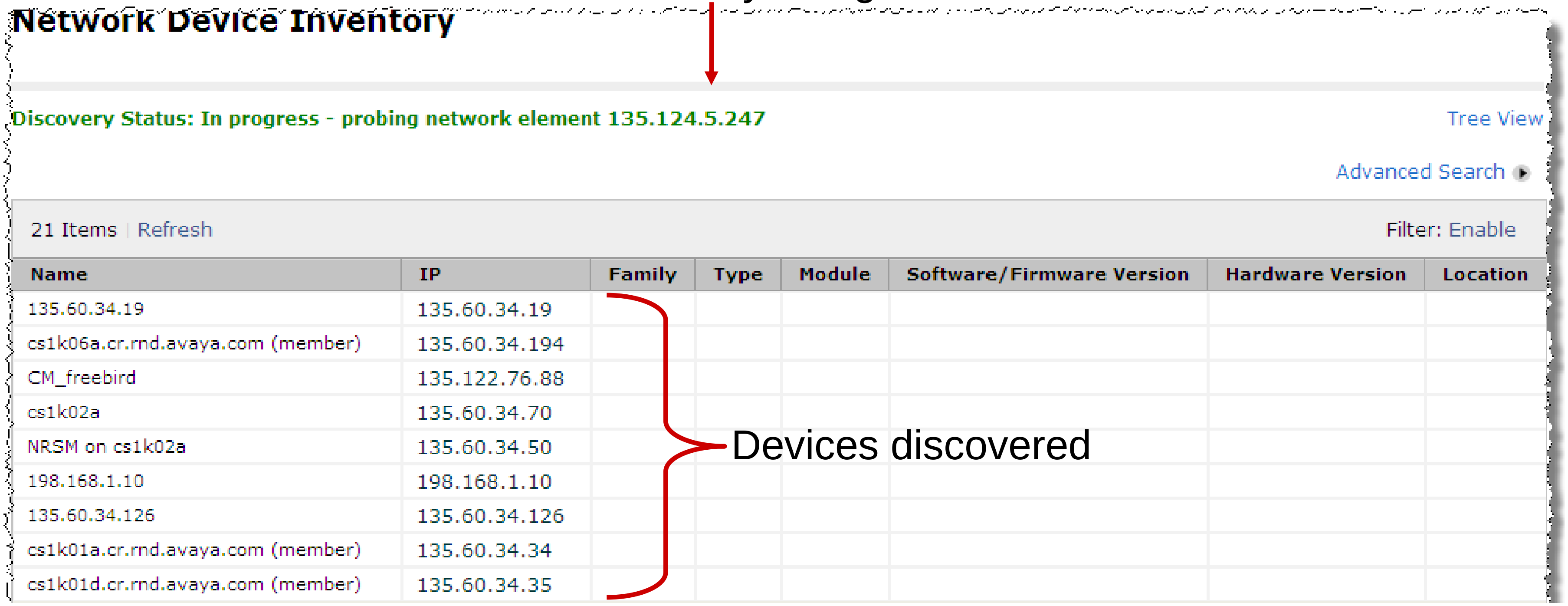
□ Clear Previous Results

To begin the inventory search:

- Select the Subnet profile to search
- Select the device type(s) to look for
- Click ‘Now’, or ‘Schedule’ for a later search

Inventory Discovery: Scan Report

IP currently being scanned



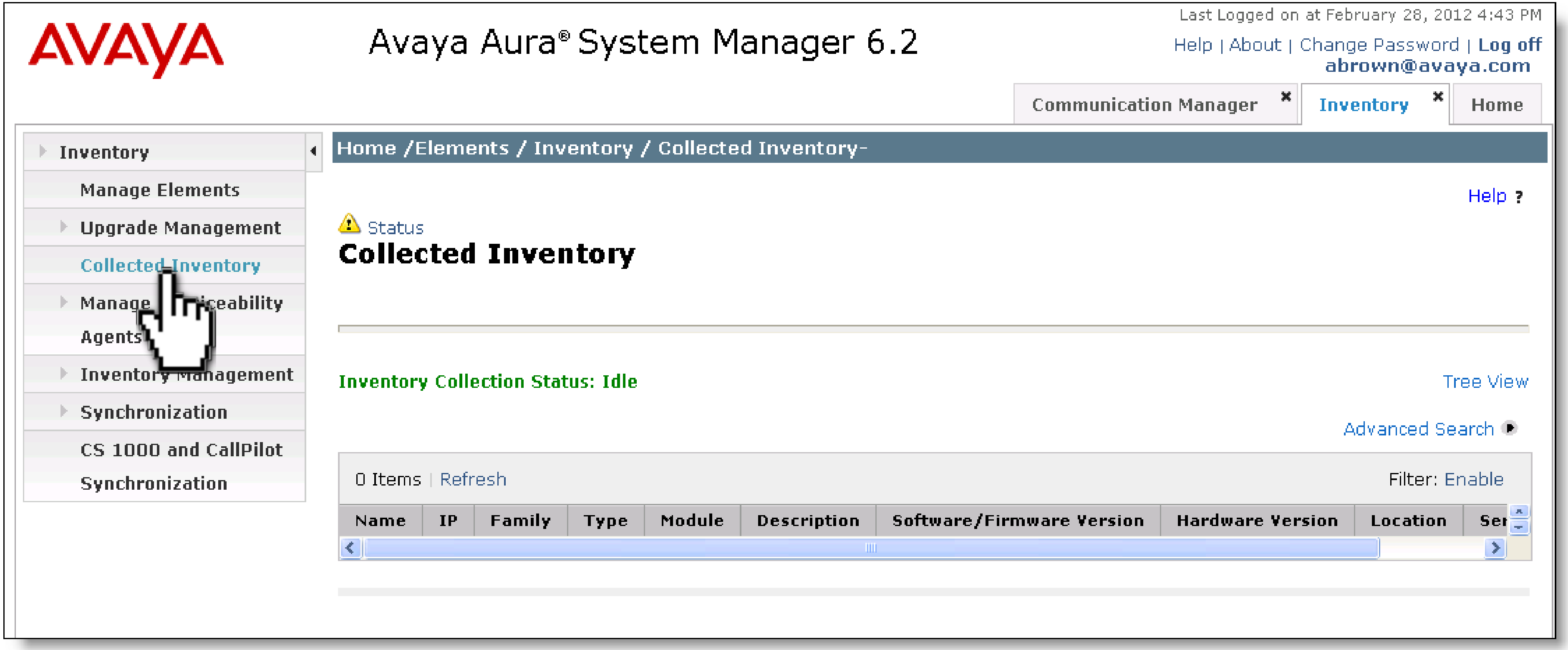
Network Device Inventory

Discovery Status: In progress - probing network element 135.124.5.247

Name	IP	Family	Type	Module	Software/Firmware Version	Hardware Version	Location
135.60.34.19	135.60.34.19						
cs1k06a.cr.rnd.avaya.com (member)	135.60.34.194						
CM_freebird	135.122.76.88						
cs1k02a	135.60.34.70						
NRSM on cs1k02a	135.60.34.50						
198.168.1.10	198.168.1.10						
135.60.34.126	135.60.34.126						
cs1k01a.cr.rnd.avaya.com (member)	135.60.34.34						
cs1k01d.cr.rnd.avaya.com (member)	135.60.34.35						

Devices discovered

Search Results: Collected Inventory



Last Logged on at February 28, 2012 4:43 PM

Avaya Aura® System Manager 6.2

Help | About | Change Password | **Log off**
abrown@avaya.com

Collected Inventory

Inventory Collection Status: Idle

0 Items | Refresh   Filter: Enable

Name	IP	Family	Type	Module	Description	Software/Firmware Version	Hardware Version	Location	Ser

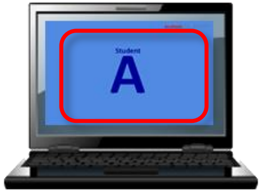
- To view the collected inventory items, click Collected Inventory.

Exercise: Discover Network Element

Objective & Outcome
The objective of this exercise is to learn how to configure SMGR to auto discover network elements. By the time you are done, SMGR should have auto discovered a CM in the training lab network.

1. Go to Home > Elements > Inventory > Inventory Management > Configuration
2. Configure SNMP Access. From SNMP Access tab click ‘New’
   – Select SNMP Type: **V1**
   – Set Read Community: **public**. Set Write Community: **public.** Click ‘***Commit***’
3. Leave optional CM Access and Gateway Access empty
4. Configure Subnet(s). From Subnets tab click ‘New’
   – Enter the subnet IP and mask of your lab: e.g. 172.16.2.0 255.255.255.0 (see student lab guide)
   – Scroll down and select the SNMP Access configuration from the list. ***Commit***.
5. Collect Inventory. Click ‘Collect Inventory’ menu link.
   – Select the network subnet to be searched, plus the type of device to search for from the lists. Click ‘Now’ to start an immediate search.
6. View Discovered items
   – Go to Collected Inventory. The discovered items should be listed.

Team Activity
Student A to drive, with student B shadowing



Student A

Student B

AVAYA | LEARNING

Module 04: Product Administration

Lesson 02: Licensing Other Services

Lesson Duration: 15 Minutes

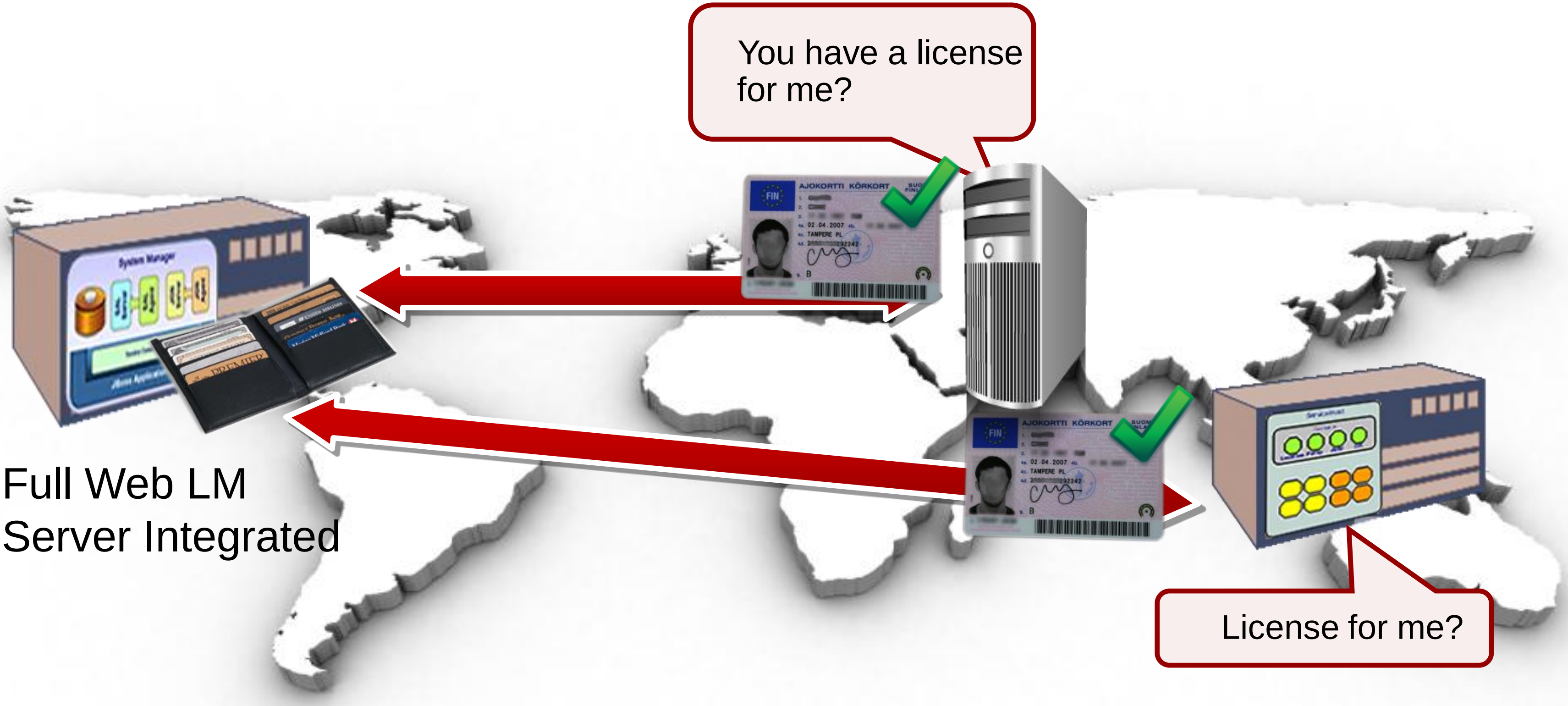
SMGR as License Manager

- Some activities require permission!
- Have to have a license
- Avaya products are just the same

Lesson Duration: 15 Minutes

SMGR Integrated WebLM Server

- Must have access to an Avaya WebLM Server before they can start properly

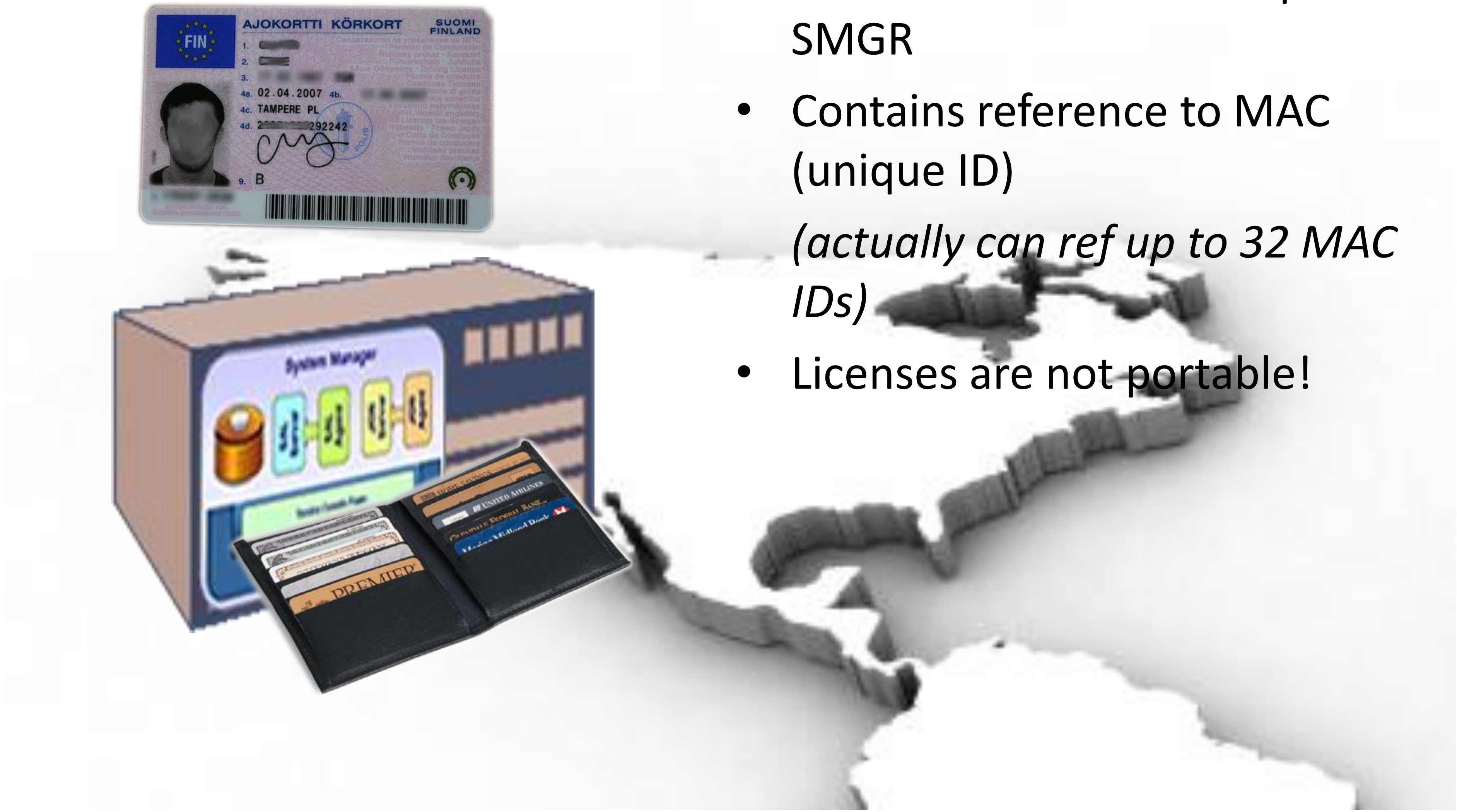


You have a license for me?

Full Web LM Server Integrated

License for me?

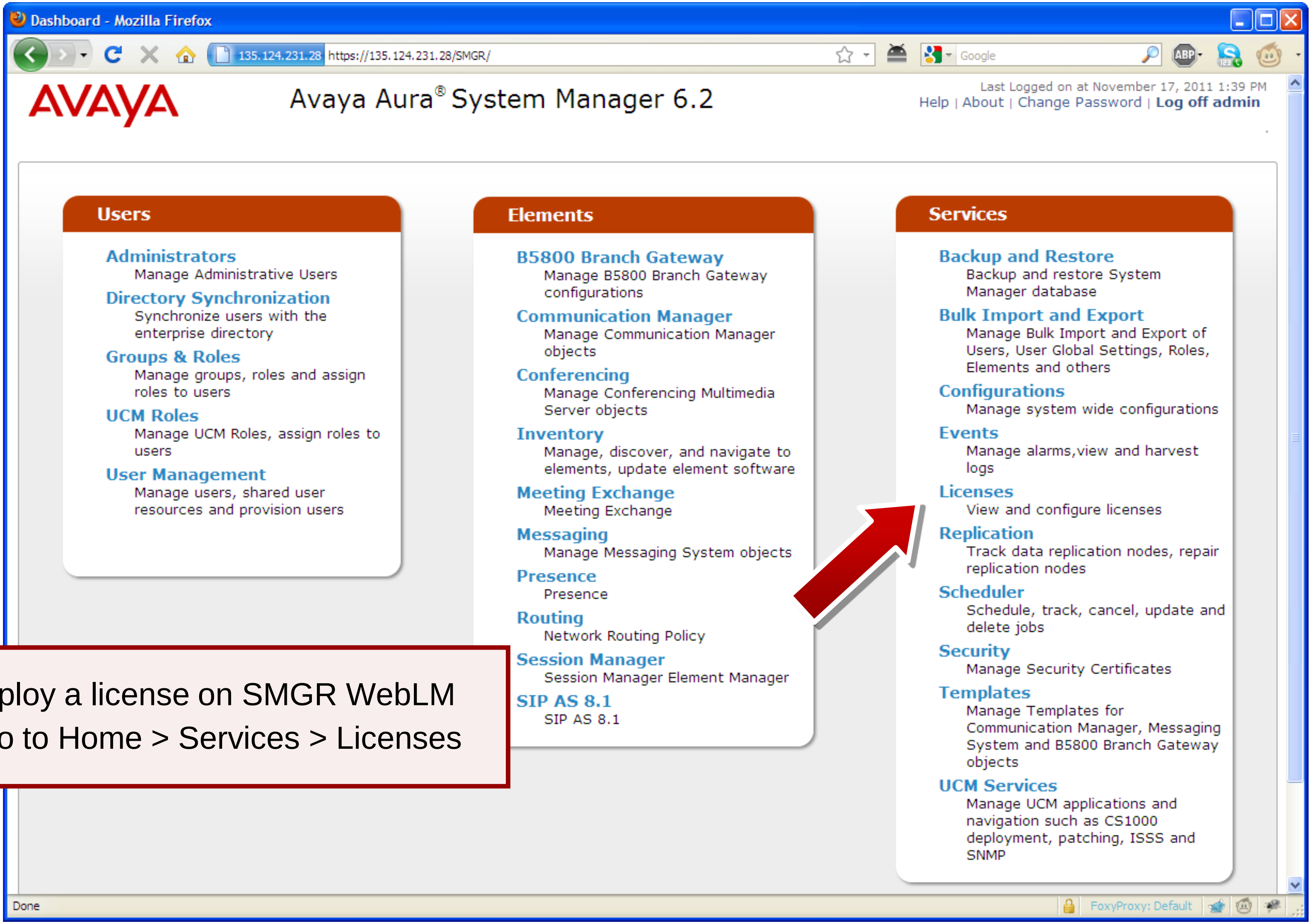
SMGR Integrated WebLM Server



- License file is bound to specific SMGR
- Contains reference to MAC (unique ID)

  (actually can ref up to 32 MAC IDs)
- Licenses are not portable!

Deploying Licenses to SMGR



AVAYA Avaya Aura® System Manager 6.2

Last Logged on at November 17, 2011 1:39 PM
Help | About | Change Password | **Log off admin**

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

UCM Roles
Manage UCM Roles, assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway configurations

Communication Manager
Manage Communication Manager objects

Conferencing
Manage Conferencing Multimedia Server objects

Inventory
Manage, discover, and navigate to elements, update element software

Meeting Exchange
Meeting Exchange

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

Scheduler
Schedule, track, cancel, update and delete jobs

Security
Manage Security Certificates

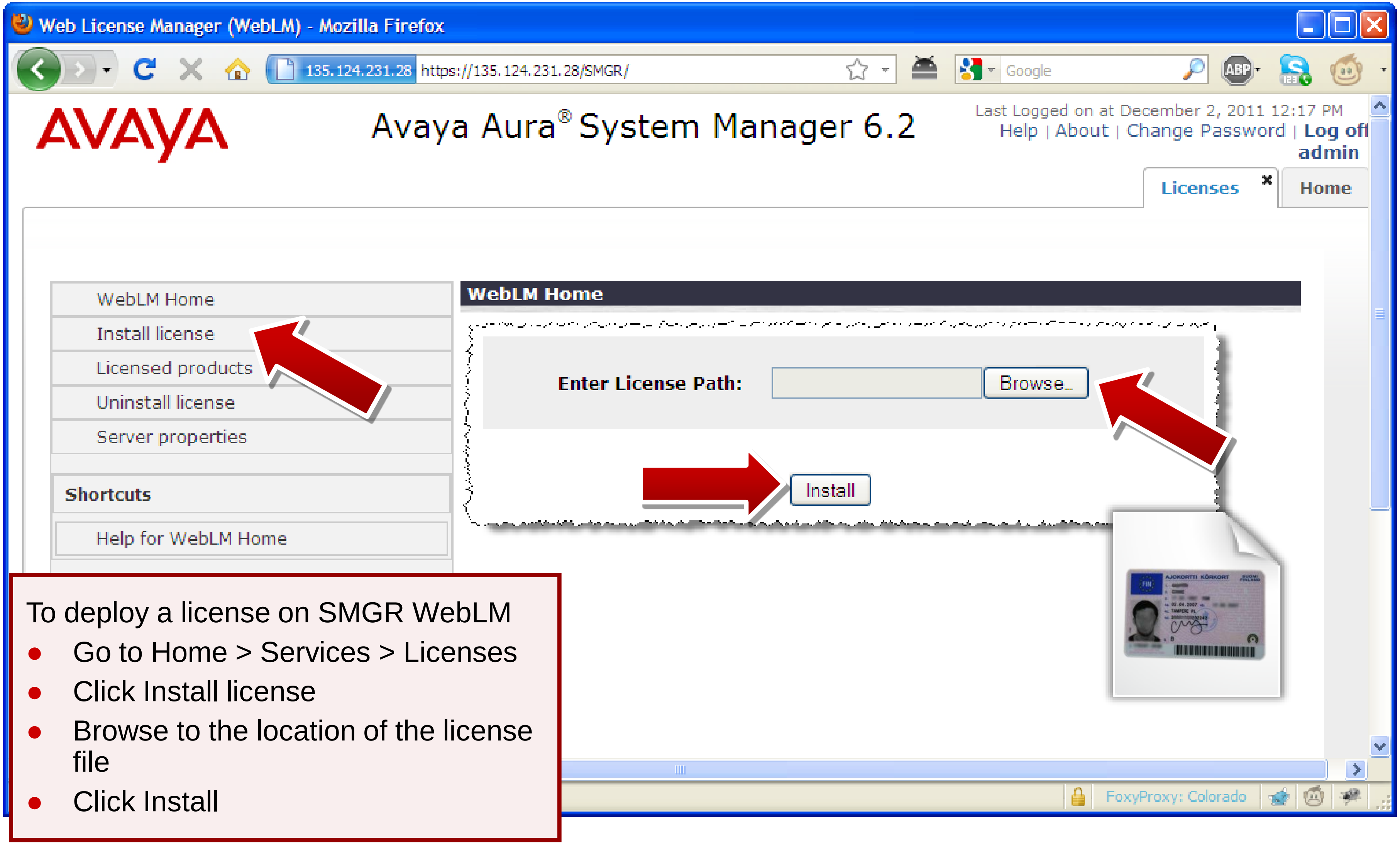
Templates
Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway objects

UCM Services
Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

To deploy a license on SMGR WebLM

- Go to Home > Services > Licenses

Deploying Licenses to SMGR (continued)



Web License Manager (WebLM) - Mozilla Firefox
135.124.231.28 https://135.124.231.28/SMGR/
Google
AVAYA
Avaya Aura® System Manager 6.2
Last Logged on at December 2, 2011 12:17 PM
Help | About | Change Password | Log off admin
Licenses
Home
WebLM Home
Install license
Licensed products
Uninstall license
Server properties
Shortcuts
Help for WebLM Home
Enter License Path:
Browse...
Install
FoxyProxy: Colorado

To deploy a license on SMGR WebLM

- Go to Home > Services > Licenses
- Click Install license
- Browse to the location of the license file
- Click Install

Exercise: Deploy a License to SMGR

Objective & Outcome
The objective of this exercise is to become familiar with the process of deploying a license in to SMGR's WebLM license repository. By the time you are done, you should have a license showing in the WebLM Home.

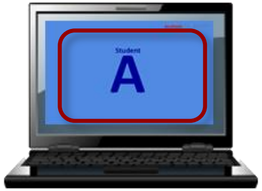
1. Check for existing licenses
   - Navigate to Home > Services > Licenses > WebLM Home
   - Check to see if any licenses are already installed

2. Install a license
   - Click link '***Install License***' from the navigation pane
   - Browse to the license file, located on your student desktop. See the student guide for file name. Click **Open**
   - The license should now be displayed in the WebLM Home list

Note:
- There is no POM server installed in the training lab – we're using POM as an example of a product
- If using a pre-generated license, deployment may fail since it's tied to the MAC of SMGR, which is generated anew on each install

POM = Proactive Outreach Manager
Used in Avaya call centers to manage automated outbound campaigns.
For more info, see:
http://www.avaya.com/usa/product/proactive-outreach-manager

Individual Exercise – both students can work simultaneously



Student A

Student B

AVAYA | LEARNING

Module 05:

Handling Data in Bulk

Module Duration: 3 Hours

Module Objectives

- After completing this module, you will be able to:
  - Import / export data to / from SMGR in bulk.

Module Duration: 45 Minutes

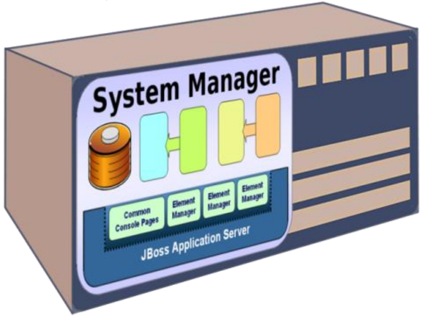
AVAYA | LEARNING

Module 05: Handling Data In Bulk

Lesson 01: Importing Data

Lesson Duration: 20 Minutes

Provisioning Manually? Administrative Headache!



SMGR will manage
large numbers of users

Lesson Duration: 20 Minutes

Importing In Bulk

- Initially provisioning an enterprise
- Moving lots information into a new Avaya Aura® installation

Supposes data must already exist somewhere!

Importing In Bulk (continued)

- Modify large batches of records
  - Company takeover – change of email addresses
  - Need to modify all of the contact centre staff application sequencing

Importing In Bulk – What can be Imported/Exported?

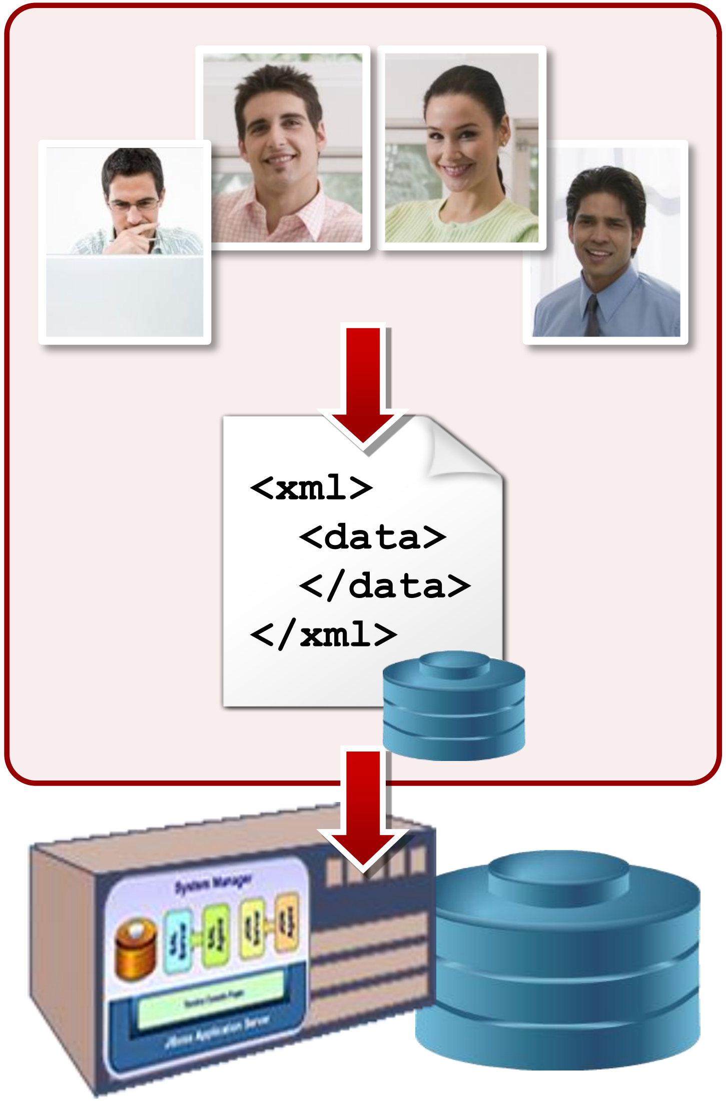
- User Profiles (Including Communication Profile)
- Application Sequencing
- Personal Contact Lists
- Shared Addresses
- Presence Access Control Lists (ACL)
- SMGR Roles
- Element Inventory Details
- Etc.

Importing In Bulk – The Process

- SMGR Data is represented as xml
- XML data can be read by SMGR and added to back in to the database repository
- SMGR doesn’t say how to create xml file – it only determines the structure of the data
  - Use of Avaya ProVision?

- Note: if the data is currently held in
  - Lotus Domino
  - Microsoft Active Directory
  - or other LDAP based backend

  The SMGR LDAP synchronisation tool should be used instead of bulk import / export



Import Performance

Initial provisioning of SMGR may involve a large dataset

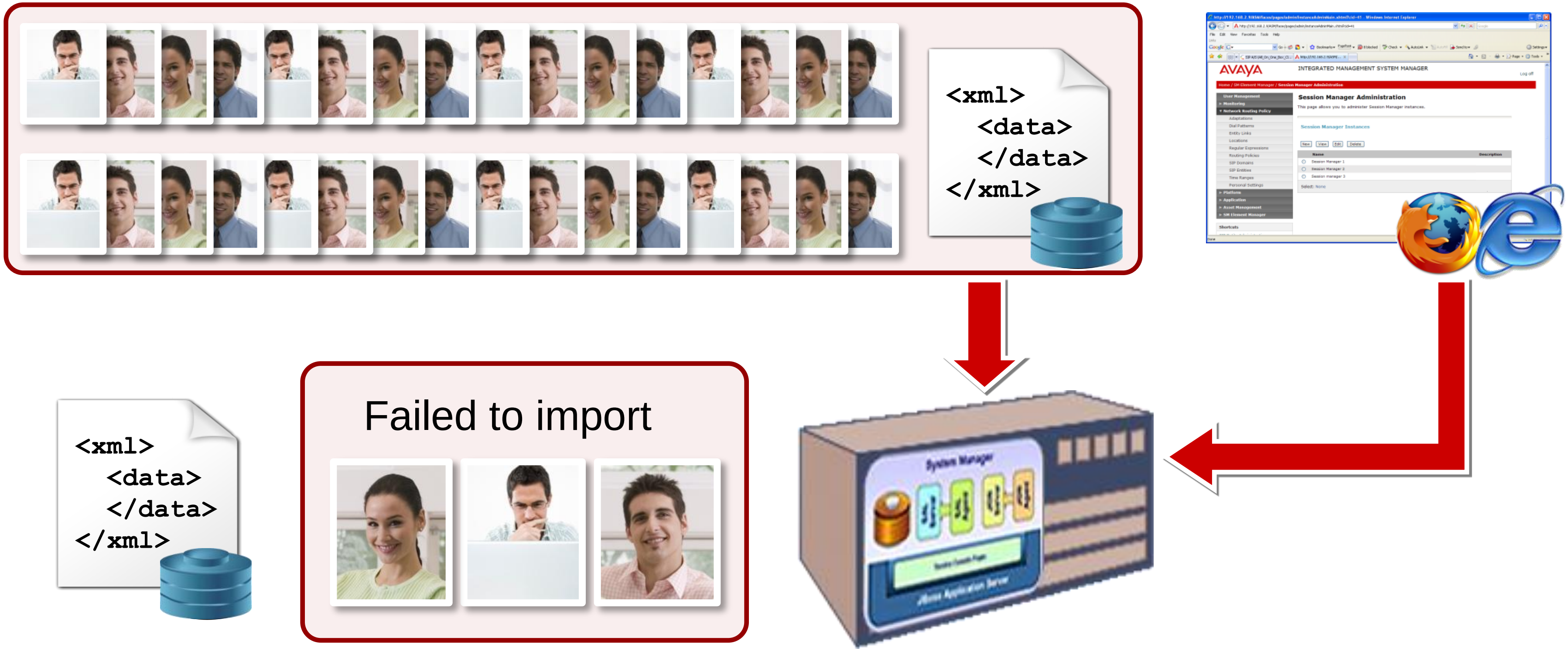
- Bulk Import supports 60 records / minute
- 5,000 Users in a single 600Mb file
- 100,000 Users max in one import – spread across multiple files of 5,000 users per file
  - Larger numbers of users can be imported, but will need to be split over multiple import tasks

```
<xml>
  <data>
  </data>
</xml>
```

```
<xml>
  <data>
  </data>
</xml>
```

Importing – Failed Records?

- Any records that fail to import are collated and offered for download through SMGR UI
- Failed records can then be analyzed, modified and re-imported
- NB: XML syntax errors will prevent import



```
<xml>
  <data>
  </data>
</xml>
```

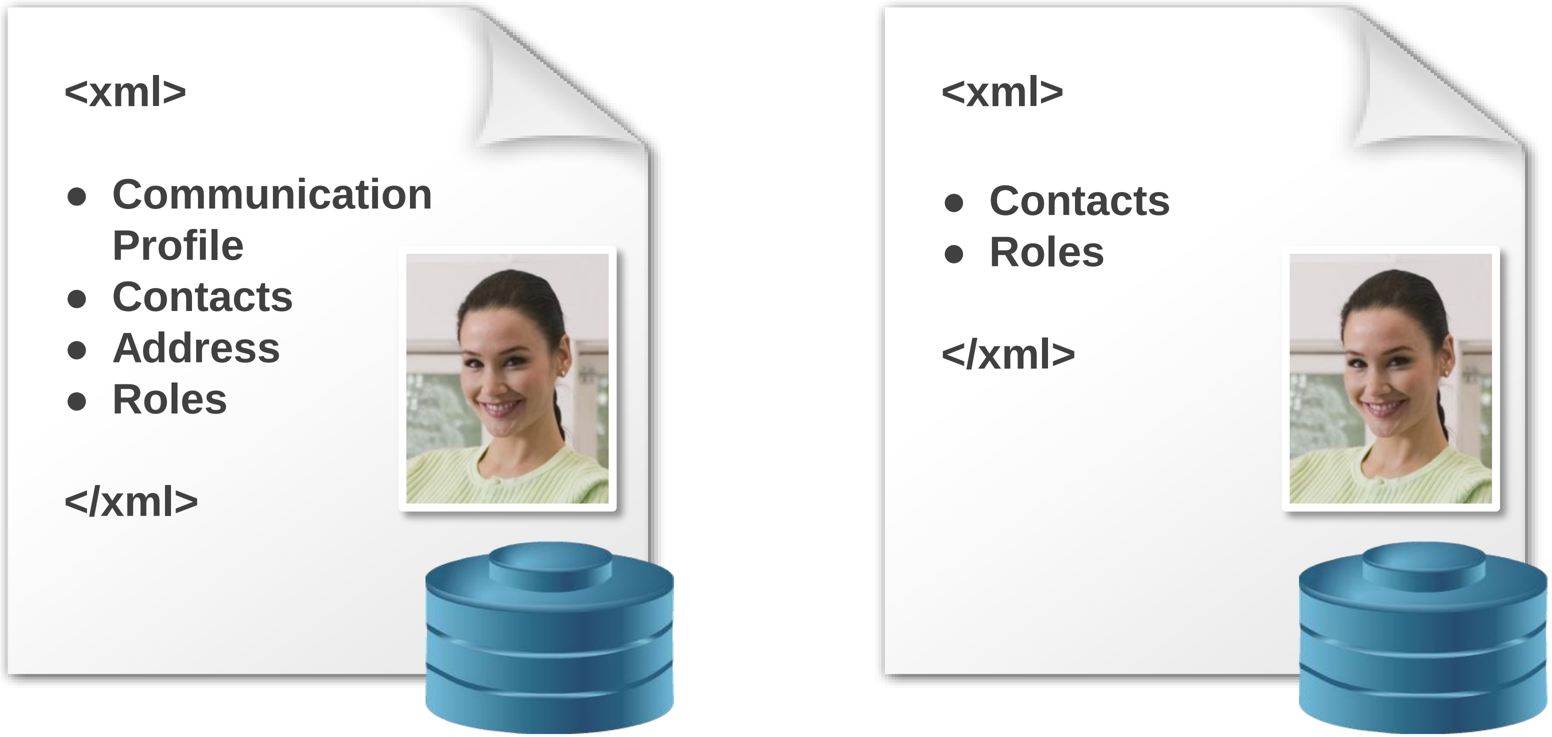
Failed to import

```
<xml>
  <data>
  </data>
</xml>
```

AVAYA
INTEGRATED MANAGEMENT SYSTEM MANAGER
Session Manager Administration
Session Manager Instances
System Manager
JBoss Application Server

Importing – Failed Records? (continued)

- SMGR supports both full and partial User data importing
- Can update existing user’s details – E.g. Add a contact



<xml>

- Communication Profile
- Contacts
- Address
- Roles

</xml>

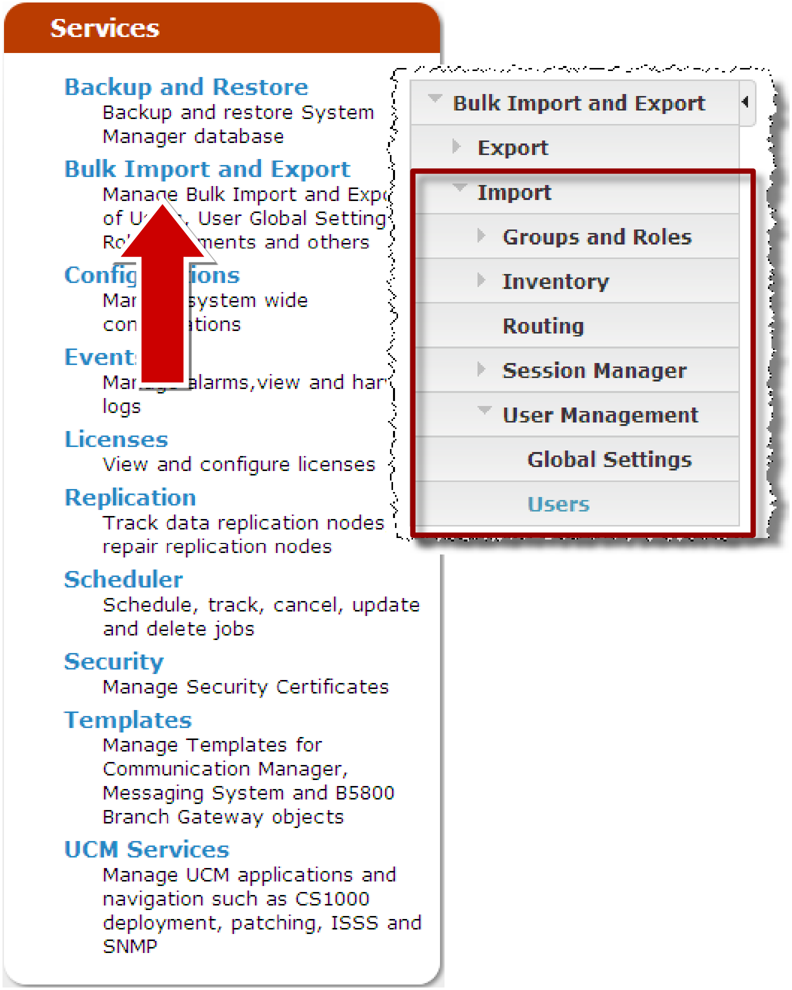
<xml>

- Contacts
- Roles

</xml>

Importing Data – 2 Ways

1. Dedicated Import / Export pages



Services

Backup and Restore
Backup and restore System Manager database

Bulk Import and Export
Manage Bulk Import and Expo of U... User Global Setting Ro... ...ments and others

Config...ions
Ma... system wide con...tions

Event...
Ma... alarms,view and har... logs

Licenses
View and configure licenses

Replication
Track data replication nodes repair replication nodes

Scheduler
Schedule, track, cancel, update and delete jobs

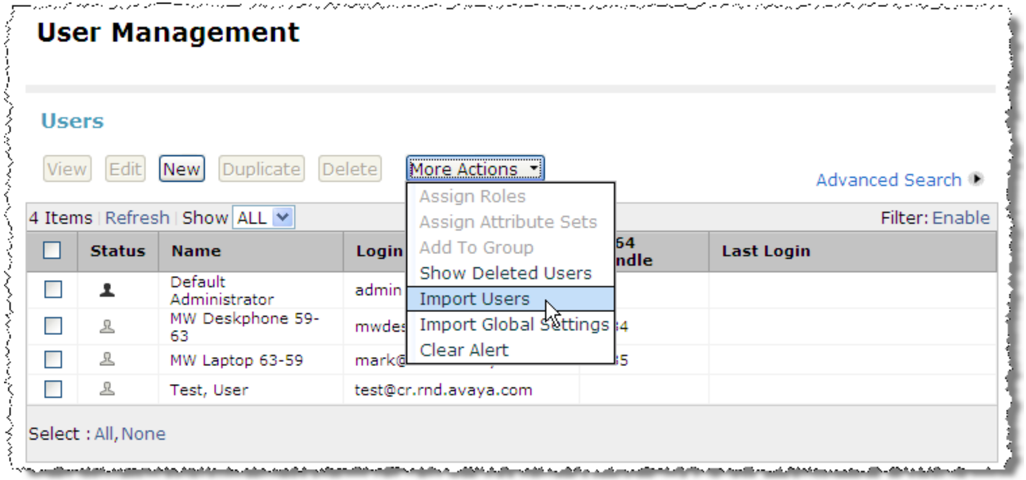
Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway objects

UCM Services
Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

- Bulk Import and Export
  - Export
  - Import
    - Groups and Roles
    - Inventory
    - Routing
    - Session Manager
    - User Management
      - Global Settings
      - Users

2. From under the relevant element manager sections



User Management

Users

View | Edit | New | Duplicate | Delete | More Actions ▾ | Advanced Search ▸

- Assign Roles
- Assign Attribute Sets
- Add To Group
- Show Deleted Users
- Import Users
- Import Global Settings
- Clear Alert

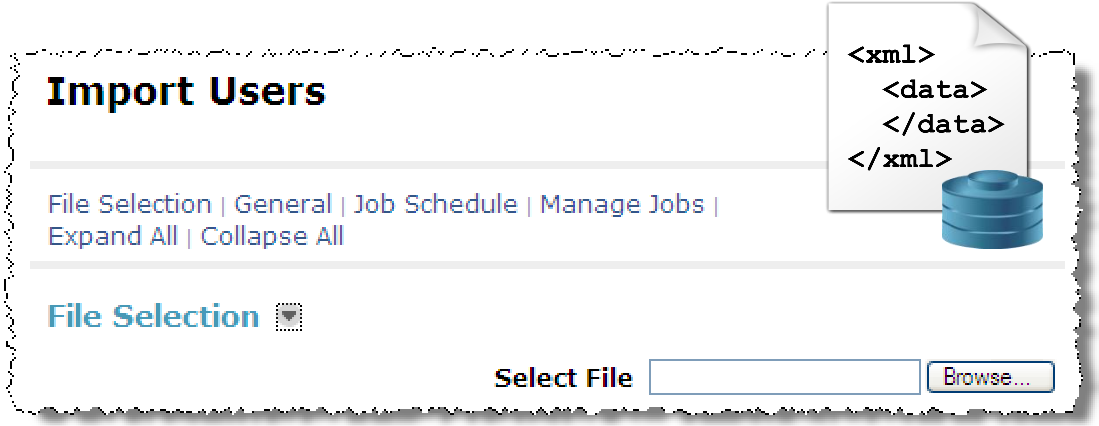
4 Items | Refresh | Show ALL ▾ Filter: Enable

□	Status	Name	Login	...64 ...ndle	Last Login
□	👤	Default Administrator	admin		
□	👤	MW Deskphone 59-63	mwdes...	...4	
□	👤	MW Laptop 63-59	mark@...	...5	
□	👤	Test, User	test@cr.rnd.avaya.com		

Select : All, None

Importing User Data

- Select import XML file
- Configure import
  - Determine error handling – what to do when a problem is encountered Abort or continue?
  - Determine if the import will be of whole records or partial records
  - Determine action when a duplicate record is found.
    - Skip
    - Merge
    - Replace
    - Delete

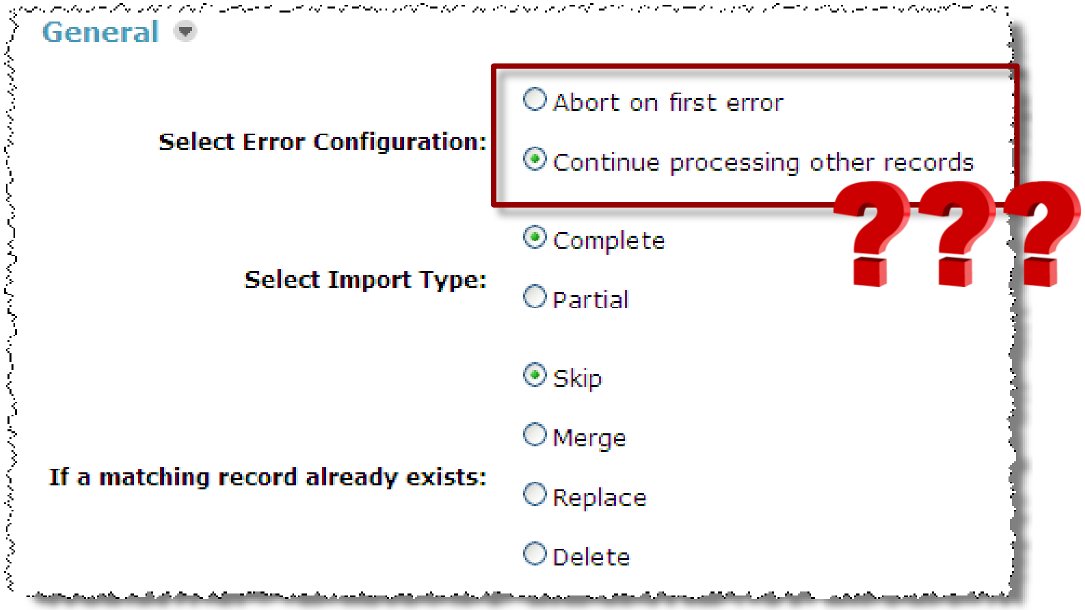


Import Users

File Selection | General | Job Schedule | Manage Jobs |
Expand All | Collapse All

File Selection

Select File [ ] Browse...



General

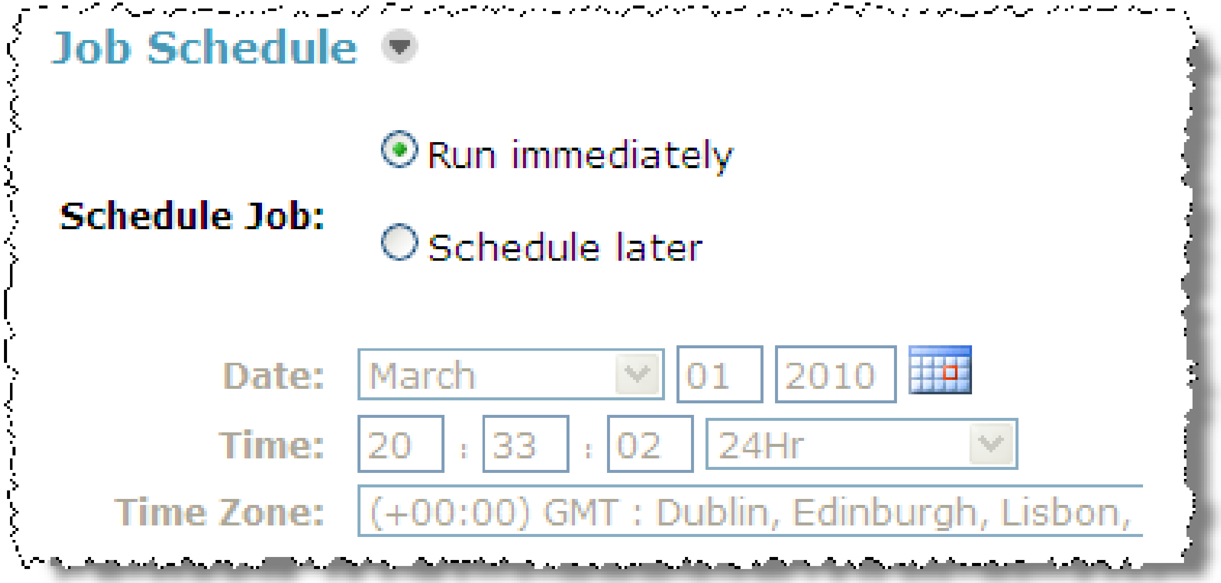
Select Error Configuration:
○ Abort on first error
● Continue processing other records

Select Import Type:
● Complete
○ Partial

If a matching record already exists:
● Skip
○ Merge
○ Replace
○ Delete

Scheduling Import of User Data

- Large imports will take time. Consider scheduling during a maintenance window.



Job Schedule

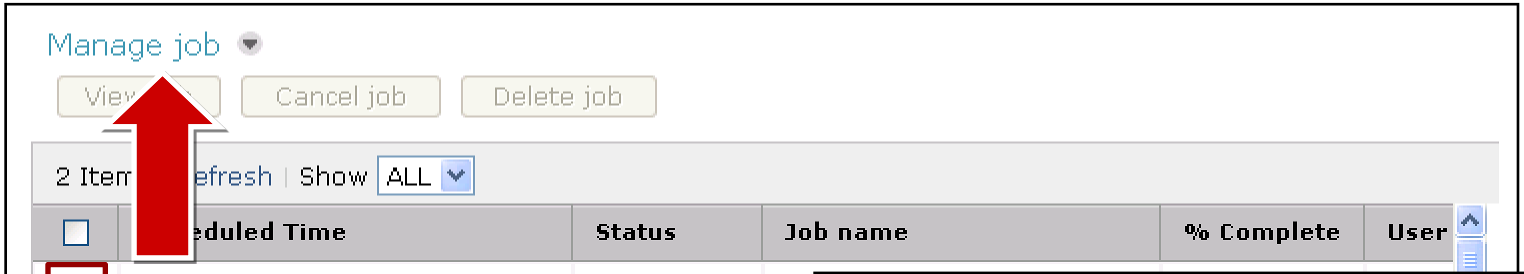
Schedule Job: ● Run immediately ○ Schedule later

Date: March 01 2010

Time: 20 : 33 : 02 24Hr

Time Zone: (+00:00) GMT : Dublin, Edinburgh, Lisbon,

Failed Records? (continued)



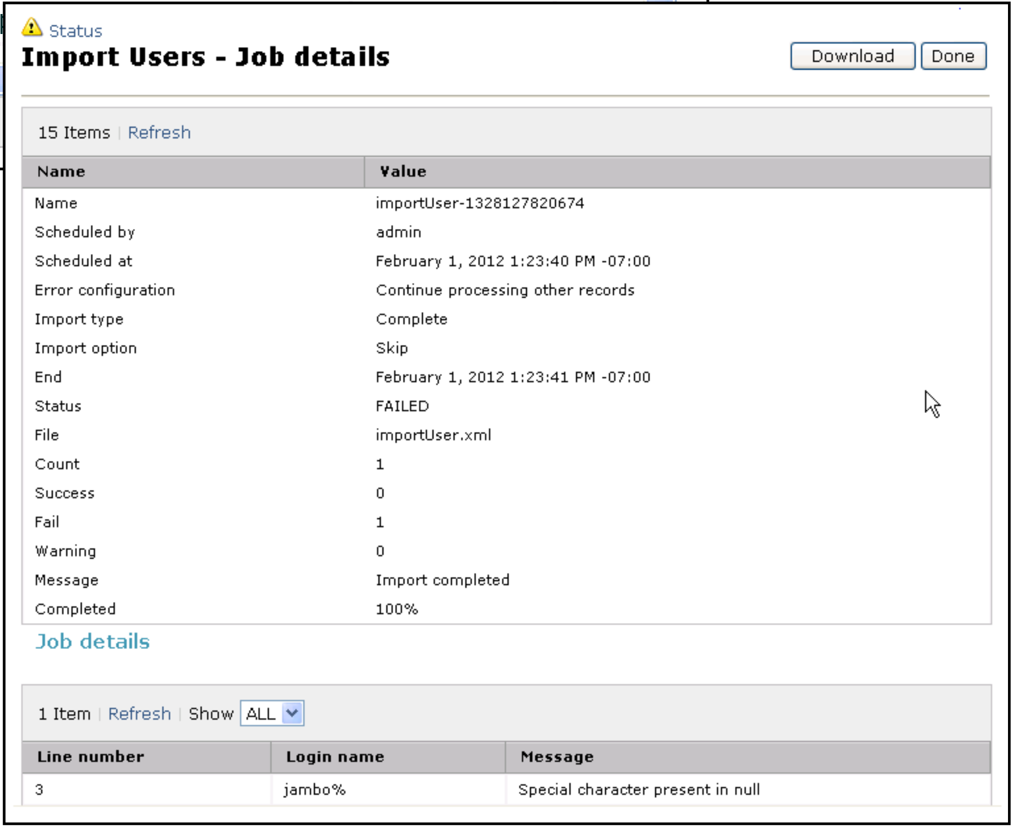
Manage job

2 Item | efresh | Show ALL

☐	eduled Time	Status	Job name	% Complete	User
☐	February 1, 2012 1:23:40 PM -07:00	FAILED	im		

Select : All, None

- Import failures will be listed
- Under ‘Manage Job’ click to view the failed job



Status

Import Users - Job details

15 Items | Refresh

Name	Value
Name	importUser-1328127820674
Scheduled by	admin
Scheduled at	February 1, 2012 1:23:40 PM -07:00
Error configuration	Continue processing other records
Import type	Complete
Import option	Skip
End	February 1, 2012 1:23:41 PM -07:00
Status	FAILED
File	importUser.xml
Count	1
Success	0
Fail	1
Warning	0
Message	Import completed
Completed	100%

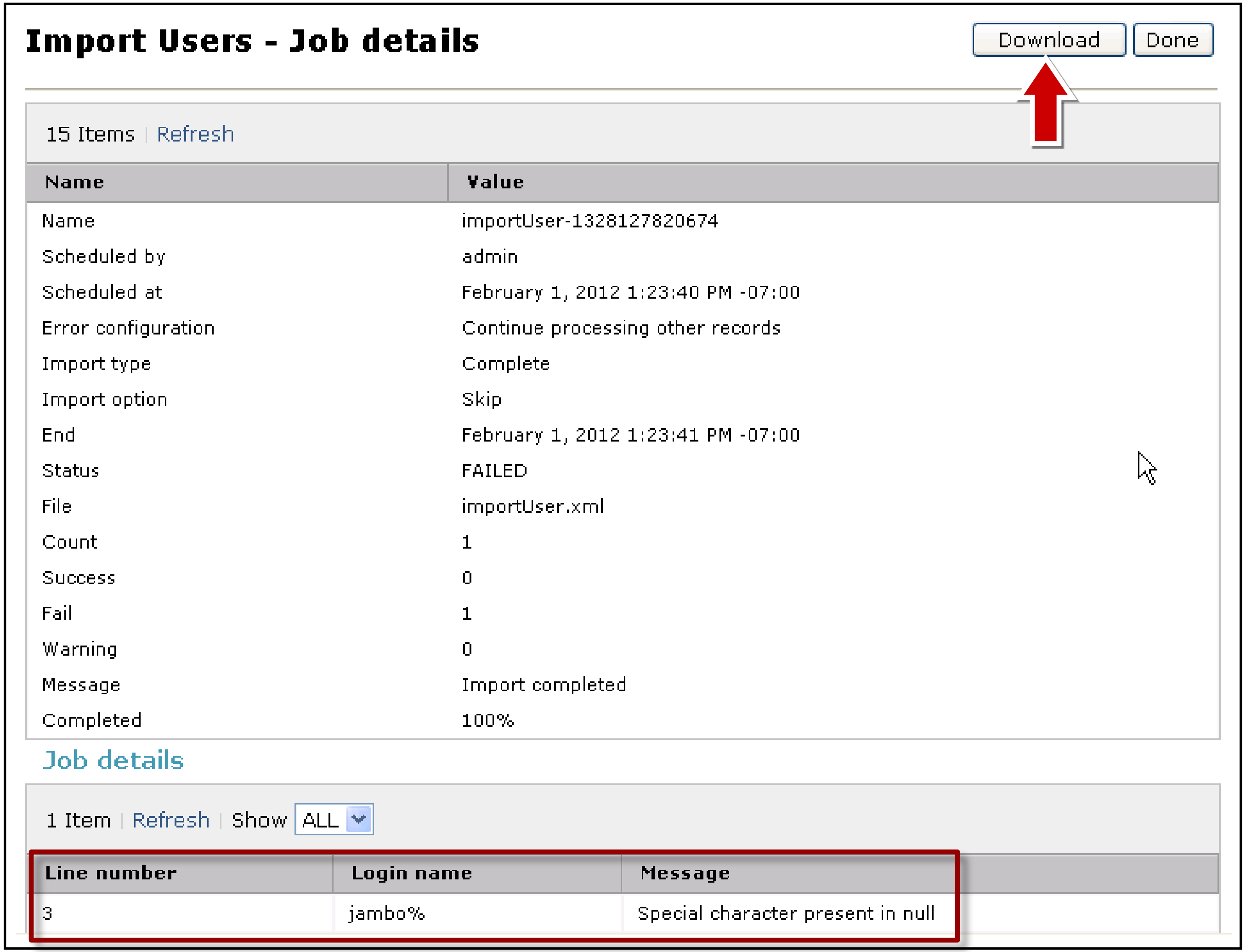
Job details

1 Item | Refresh | Show ALL

Line number	Login name	Message
3	jambo%	Special character present in null

Failed Records?

- Job details page will summarize important information
- Dialog at bottom will show where & what errors occurred
- Click to 'Download' failed records



Import Users - Job details

15 Items | Refresh

Name	Value
Name	importUser-1328127820674
Scheduled by	admin
Scheduled at	February 1, 2012 1:23:40 PM -07:00
Error configuration	Continue processing other records
Import type	Complete
Import option	Skip
End	February 1, 2012 1:23:41 PM -07:00
Status	FAILED
File	importUser.xml
Count	1
Success	0
Fail	1
Warning	0
Message	Import completed
Completed	100%

Job details

1 Item | Refresh | Show ALL

Line number	Login name	Message
3	jambo%	Special character present in null

Exercise: Bulk Import Users

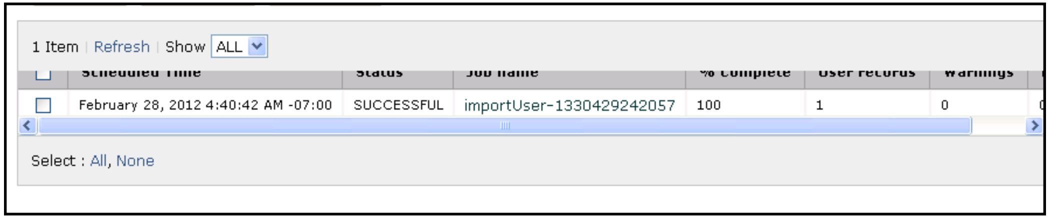
Objective & Outcome
The objective of this exercise is to learn the process of using bulk import. By the time you are done, you should have imported an additional user.

1. Navigate to Home > Services > Bulk Import and Export > Import > User Management > Users
2. Select the import file. Browse to '**importUser.xml**' file on the desktop
3. Configure import options
   - Choose to ***Continue processing other records on failure***
   - Select ***Complete Import***
   - If the user already exists, select to ***Replace*** it with the new one
   - Import immediately (don't schedule)
4. Import the users. Click **Import**
5. Check success
   - Periodically refresh the Manage Job pane. Look for '*Successful*' status
   - Check the list of users and locate the newly imported user

Team Activity
Student B to drive, with student A shadowing

Student A

Student B



1 Item | Refresh | Show ALL

□	Scheduled Time	Status	Job name	% Complete	User records	Warnings
□	February 28, 2012 4:40:42 AM -07:00	SUCCESSFUL	importUser-1330429242057	100	1	0

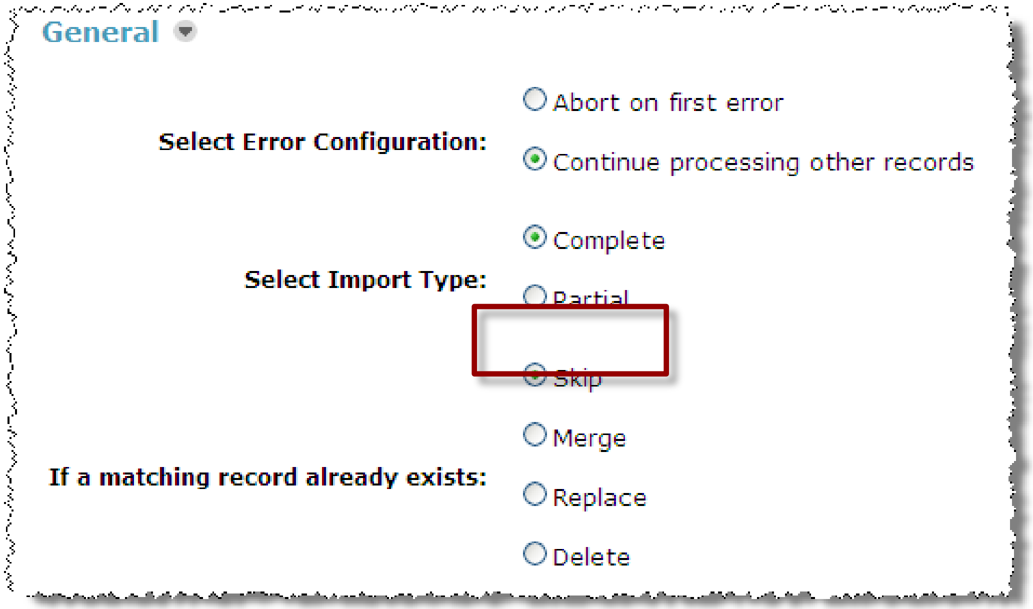
Select : All, None

Question

- On processing a record that cannot be imported, will SMGR rollback?

Importing User Data

- There is no 'roll-back' after successful import – each record is handled individually
- Consider a batch import where some records fail due to bad data
  - After correcting the data, rather than rolling back to pre-import state, re-run the import with Skip selected. Any records that imported correctly the first time will be skipped.



General

Select Error Configuration:
○ Abort on first error
● Continue processing other records

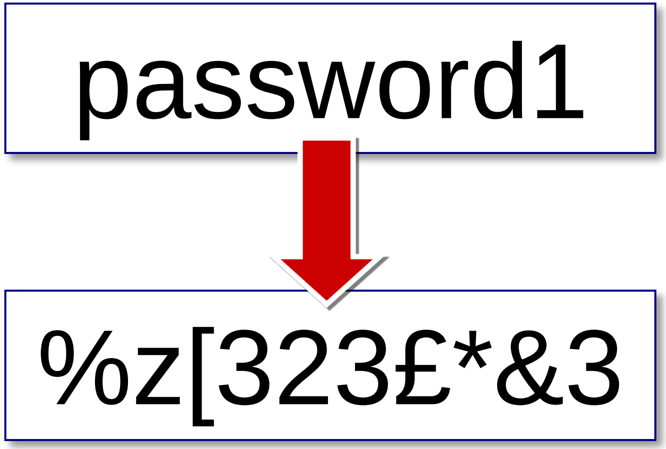
Select Import Type:
● Complete
○ Partial

If a matching record already exists:
● Skip
○ Merge
○ Replace
○ Delete

Importing User Data (continued)

- Sensitive information (user's passwords) can be supplied in the user data XML
- SMGR can handle encrypted data, deciphering encoder data before adding to the database
  - Helps keep data safe whilst moving in file format

Encrypt Utility
um_bulkimport-encryptUtil.zip


password1

%z[323£*&3

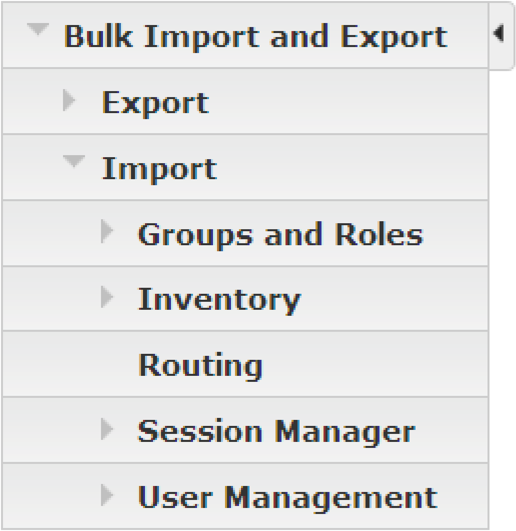
For further instructions on encrypting import passwords, see the appendix.

Importing User Data – Some Useful Info

- Login name treated as unique identifier
  - As such, 'loginname' cannot be updated by bulk import
  - If loginname matches existing record – SMGR will either replace, skip or delete that record depending on how the import is configured
- SMGR data often references other data in the system – import order matters!
- If importing users, roles & contacts:
  1. Roles
  2. Public Contacts | Shared Contacts
  3. Users
- If importing Presence ACL:
  1. Users
  2. Presence Data

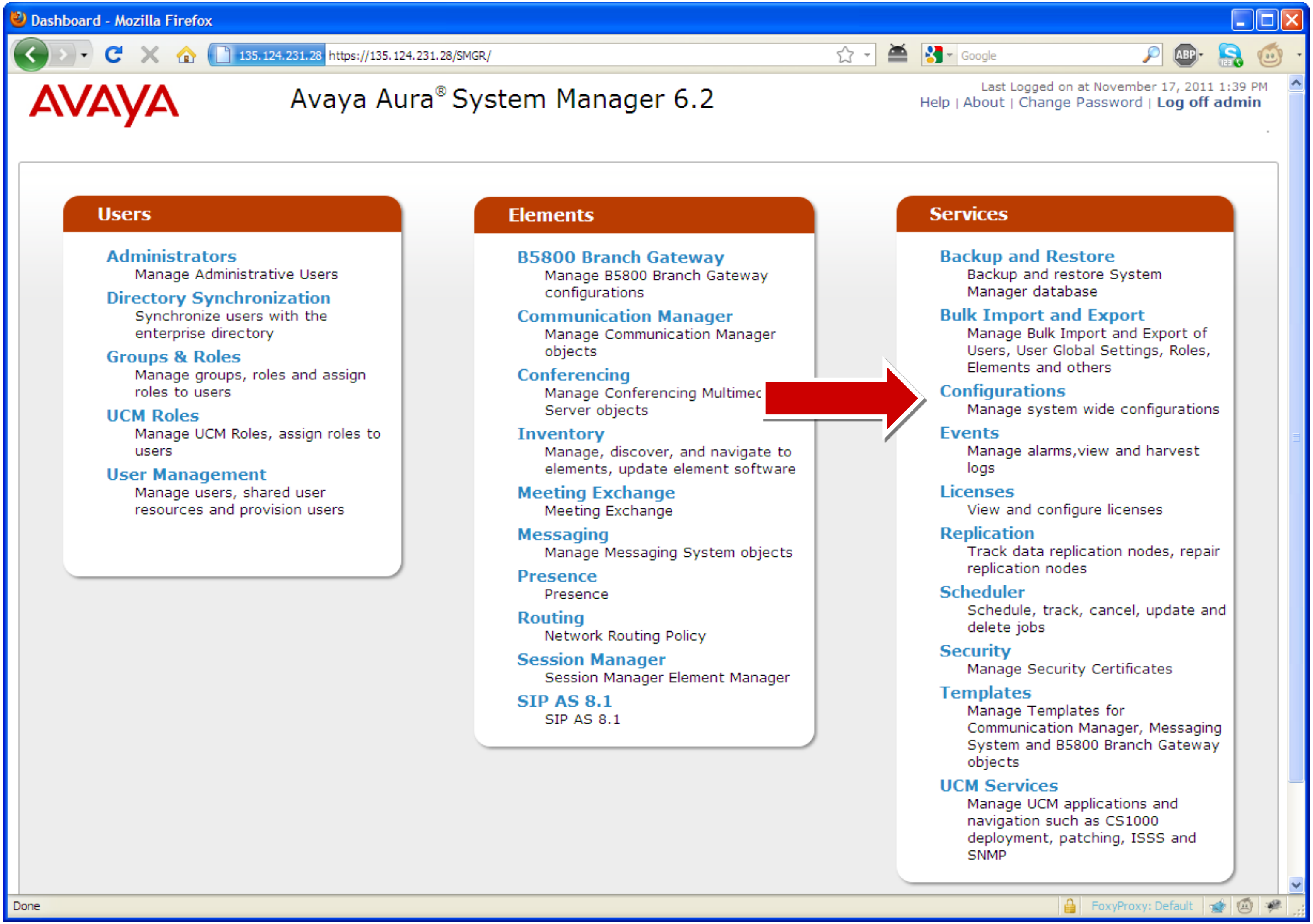
Importing: Other SMGR Data

- Other SMGR data can also be imported in similar fashion
- Inventory, Roles, Routing policies etc.



Useful since partners / professional services may want to provision as much as possible in advance of going on site to complete deployment

Configuring Default Import Options (& Other Defaults)



Dashboard - Mozilla Firefox
135.124.231.28 https://135.124.231.28/SMGR/
Google
AVAYA
Done
FoxyProxy: Default

Avaya Aura® System Manager 6.2

Last Logged on at November 17, 2011 1:39 PM

Help | About | Change Password | Log off admin

Users

- **Administrators** – Manage Administrative Users
- **Directory Synchronization** – Synchronize users with the enterprise directory
- **Groups & Roles** – Manage groups, roles and assign roles to users
- **UCM Roles** – Manage UCM Roles, assign roles to users
- **User Management** – Manage users, shared user resources and provision users

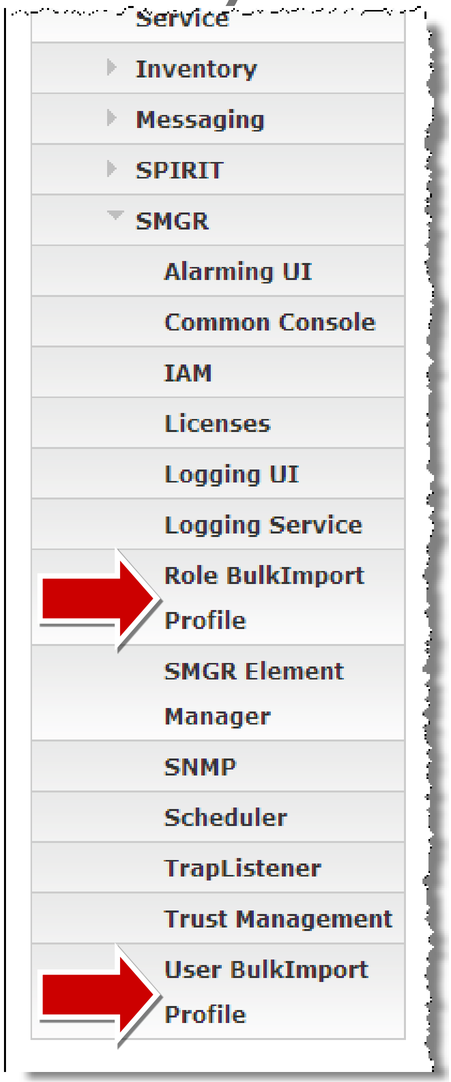
Elements

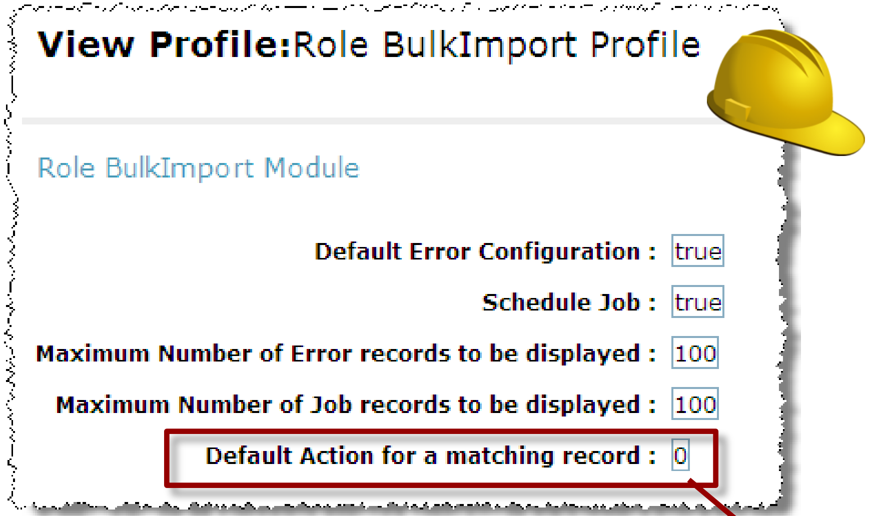
- **B5800 Branch Gateway** – Manage B5800 Branch Gateway configurations
- **Communication Manager** – Manage Communication Manager objects
- **Conferencing** – Manage Conferencing Multimed Server objects
- **Inventory** – Manage, discover, and navigate to elements, update element software
- **Meeting Exchange** – Meeting Exchange
- **Messaging** – Manage Messaging System objects
- **Presence** – Presence
- **Routing** – Network Routing Policy
- **Session Manager** – Session Manager Element Manager
- **SIP AS 8.1** – SIP AS 8.1

Services

- **Backup and Restore** – Backup and restore System Manager database
- **Bulk Import and Export** – Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others
- **Configurations** – Manage system wide configurations
- **Events** – Manage alarms,view and harvest logs
- **Licenses** – View and configure licenses
- **Replication** – Track data replication nodes, repair replication nodes
- **Scheduler** – Schedule, track, cancel, update and delete jobs
- **Security** – Manage Security Certificates
- **Templates** – Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway objects
- **UCM Services** – Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

Configuring Default Import Options (& Other Defaults) (continued)





View Profile: Role BulkImport Profile

Role BulkImport Module

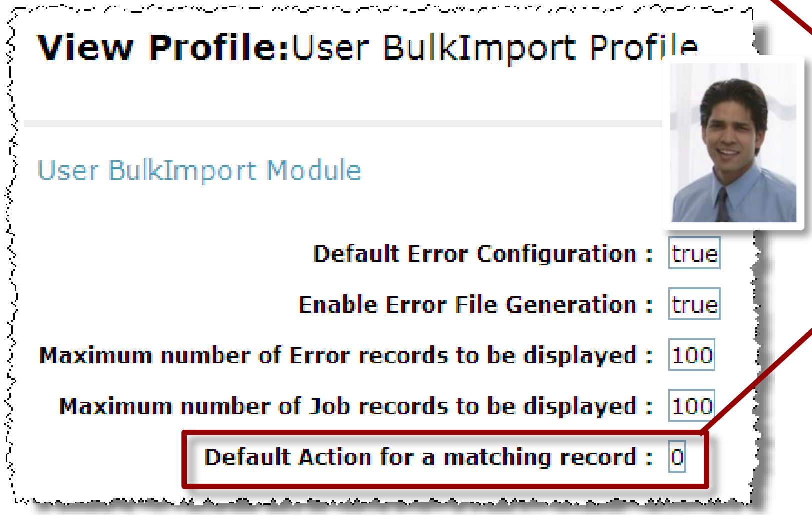
Default Error Configuration : true

Schedule Job : true

Maximum Number of Error records to be displayed : 100

Maximum Number of Job records to be displayed : 100

Default Action for a matching record : 0



View Profile: User BulkImport Profile

User BulkImport Module

Default Error Configuration : true

Enable Error File Generation : true

Maximum number of Error records to be displayed : 100

Maximum number of Job records to be displayed : 100

Default Action for a matching record : 0

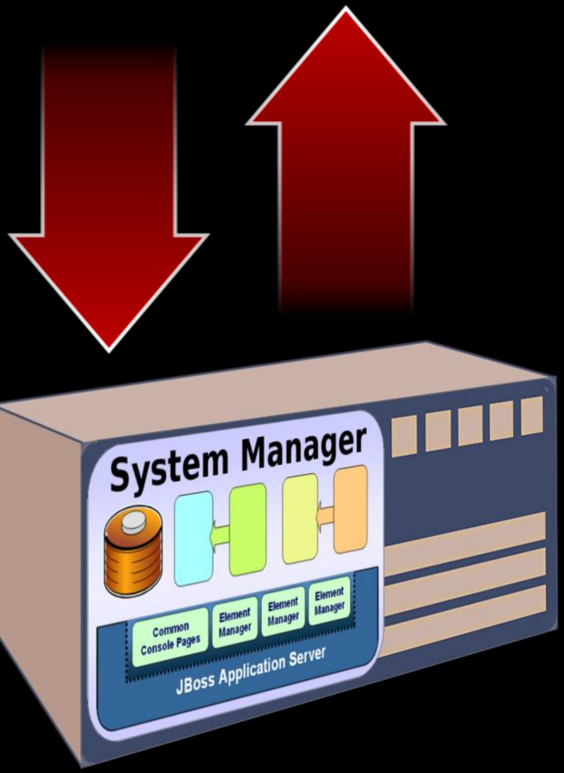
0 = Skip
1 = Merge
2 = Replace
3 = Delete

AVAYA | LEARNING

Module 05: Handling Data In Bulk

Lesson 02: Exporting Data

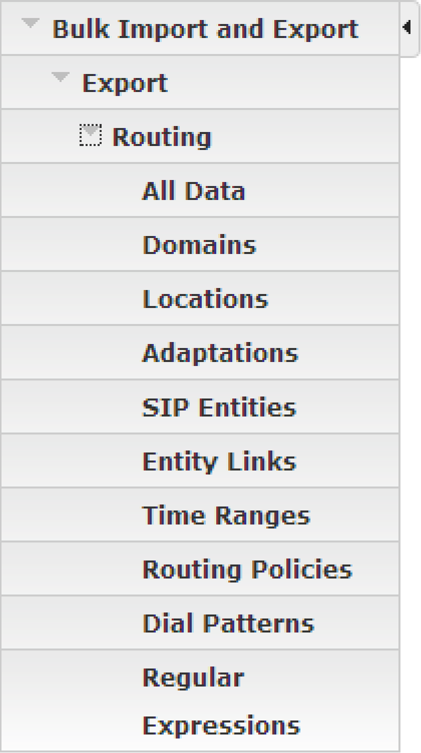
Lesson Duration: 20 minutes



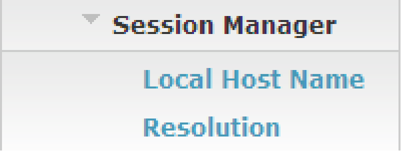
Lesson Duration: 20 Minutes

Exporting SMGR Data – 2 Export Mechanisms

- Some data may be exported via the SMGR menus

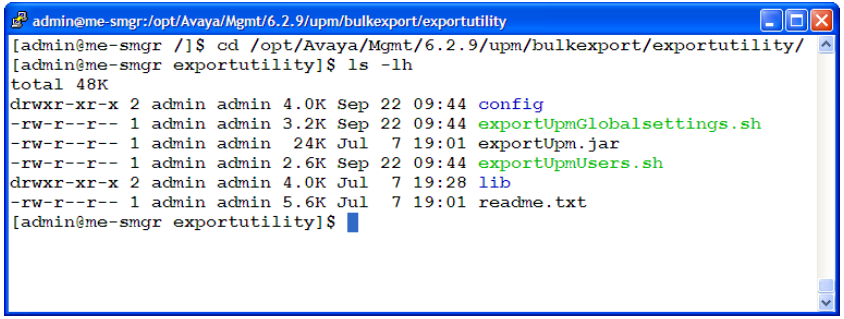


Routing Info



SM host resolution table

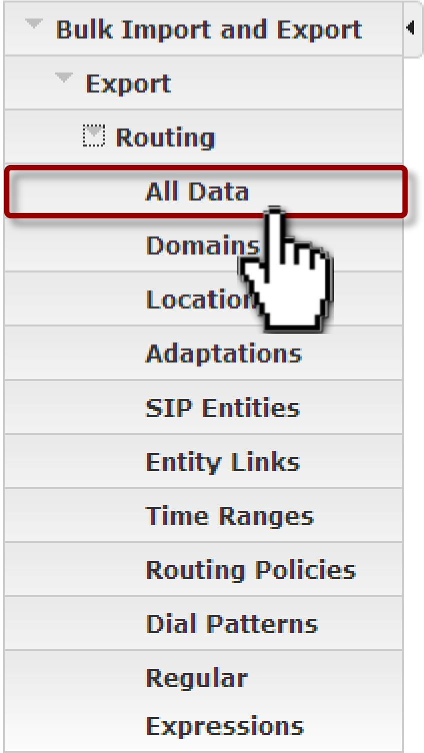
- Other data, such as Roles and Users may be exported from the command line


admin@me-smgr:/opt/Avaya/Mgmt/6.2.9/upm/bulkexport/exportutility

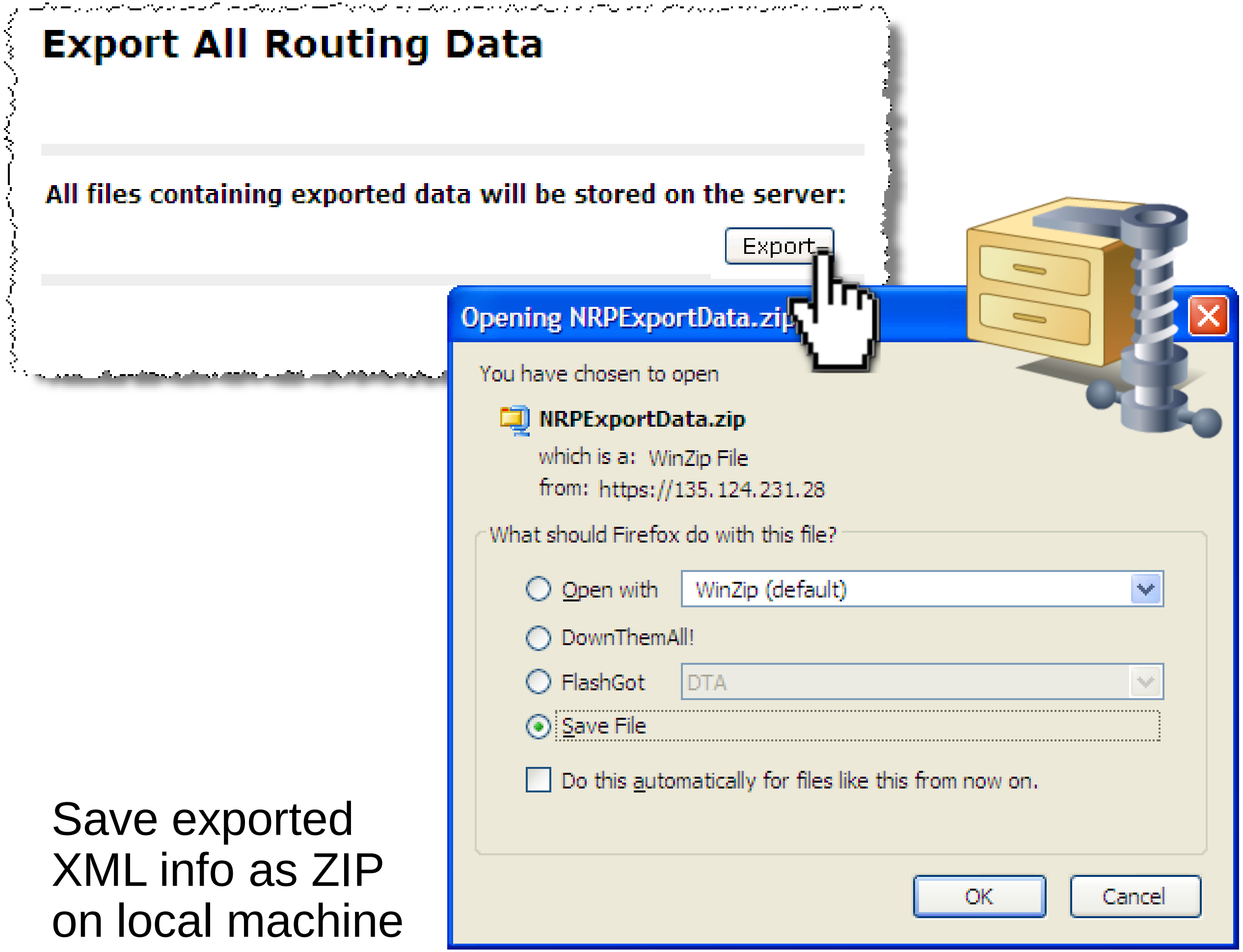
```
[admin@me-smgr /]$ cd /opt/Avaya/Mgmt/6.2.9/upm/bulkexport/exportutility/
[admin@me-smgr exportutility]$ ls -lh
total 48K
drwxr-xr-x 2 admin admin 4.0K Sep 22 09:44 config
-rw-r--r-- 1 admin admin 3.2K Sep 22 09:44 exportUpmGlobalsettings.sh
-rw-r--r-- 1 admin admin  24K Jul  7 19:01 exportUpm.jar
-rw-r--r-- 1 admin admin 2.6K Sep 22 09:44 exportUpmUsers.sh
drwxr-xr-x 2 admin admin 4.0K Jul  7 19:28 lib
-rw-r--r-- 1 admin admin 5.6K Jul  7 19:01 readme.txt
[admin@me-smgr exportutility]$ 
```

Exporting SMGR Data

- Exporting data via the web interface packages records into zip files.



Bulk Import and Export
- Export
  - Routing
    - All Data
    - Domains
    - Locations
    - Adaptations
    - SIP Entities
    - Entity Links
    - Time Ranges
    - Routing Policies
    - Dial Patterns
    - Regular Expressions



Export All Routing Data

All files containing exported data will be stored on the server:

Export

Opening NRPExportData.zip

You have chosen to open

NRPExportData.zip

which is a: WinZip File

from: https://135.124.231.28

What should Firefox do with this file?

○ Open with WinZip (default)

○ DownThemAll!

○ FlashGot DTA

● Save File

□ Do this automatically for files like this from now on.

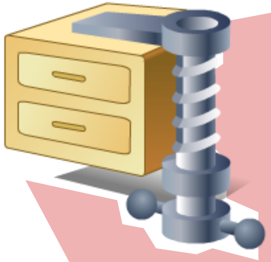
OK Cancel

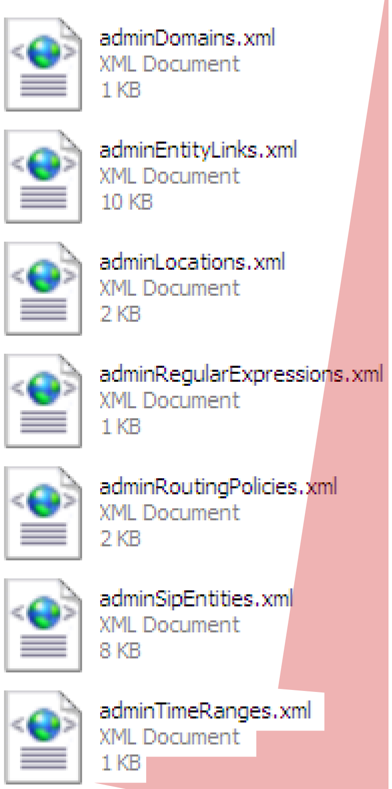
Save exported XML info as ZIP on local machine

Exporting SMGR Data (continued)

- The exported ZIP file may be extracted and its xml files viewed.

NRPExportData.zip





adminDomains.xml
XML Document
1 KB

adminEntityLinks.xml
XML Document
10 KB

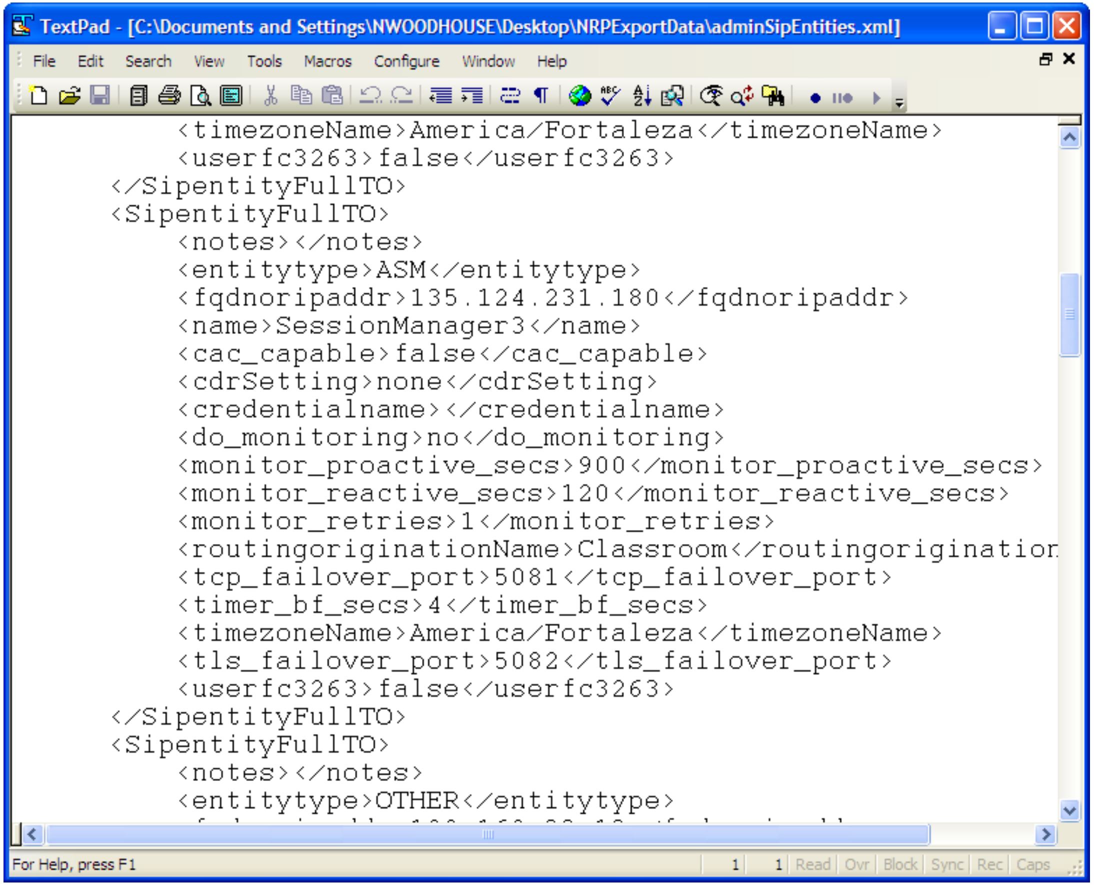
adminLocations.xml
XML Document
2 KB

adminRegularExpressions.xml
XML Document
1 KB

adminRoutingPolicies.xml
XML Document
2 KB

adminSipEntities.xml
XML Document
8 KB

adminTimeRanges.xml
XML Document
1 KB



TextPad - [C:\Documents and Settings\NWOODHOUSE\Desktop\NRPExportData\adminSipEntities.xml]
File
Edit
Search
View
Tools
Macros
Configure
Window
Help
For Help, press F1
1
1
Read
Ovr
Block
Sync
Rec
Caps

```
        <timezoneName>America/Fortaleza</timezoneName>
        <userfc3263>false</userfc3263>
    </SipentityFullTO>
    <SipentityFullTO>
        <notes></notes>
        <entitytype>ASM</entitytype>
        <fqdnoripaddr>135.124.231.180</fqdnoripaddr>
        <name>SessionManager3</name>
        <cac_capable>false</cac_capable>
        <cdrSetting>none</cdrSetting>
        <credentialname></credentialname>
        <do_monitoring>no</do_monitoring>
        <monitor_proactive_secs>900</monitor_proactive_secs>
        <monitor_reactive_secs>120</monitor_reactive_secs>
        <monitor_retries>1</monitor_retries>
        <routingoriginationName>Classroom</routingorigination
        <tcp_failover_port>5081</tcp_failover_port>
        <timer_bf_secs>4</timer_bf_secs>
        <timezoneName>America/Fortaleza</timezoneName>
        <tls_failover_port>5082</tls_failover_port>
        <userfc3263>false</userfc3263>
    </SipentityFullTO>
    <SipentityFullTO>
        <notes></notes>
        <entitytype>OTHER</entitytype>
```

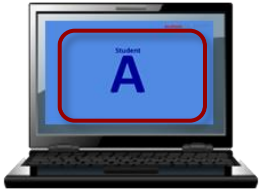
Exercise: Export All Routing Data

Objective & Outcome

The objective of this exercise is to learn how to export SMGR data using the Web Interface. By the time you are done, you should have an exported ZIP file that contains xml file(s) that represent SMGR routing policies and surround data.

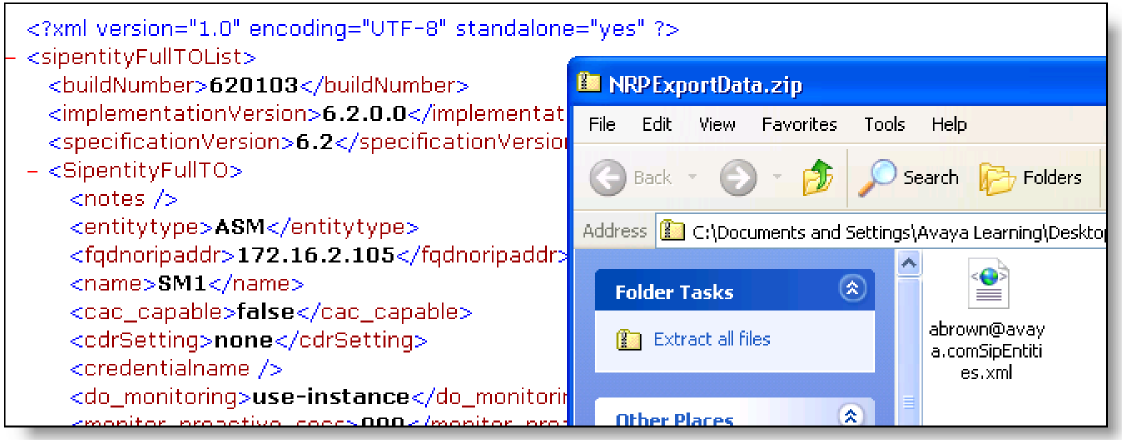
1. Navigate to Home > Services > Bulk Import and Export > Export > Routing > All Data.
2. Click ***Export***. Select ***Save*** and choose the local desktop as the save location. Save the exported file.
3. Navigate to the student desktop and open the ZIP file. Examine content

Team Activity
Student A to drive,
with student B
shadowing



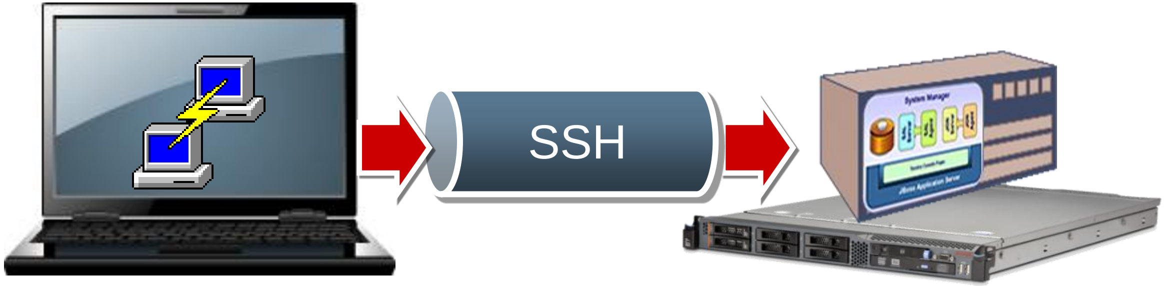
Student A

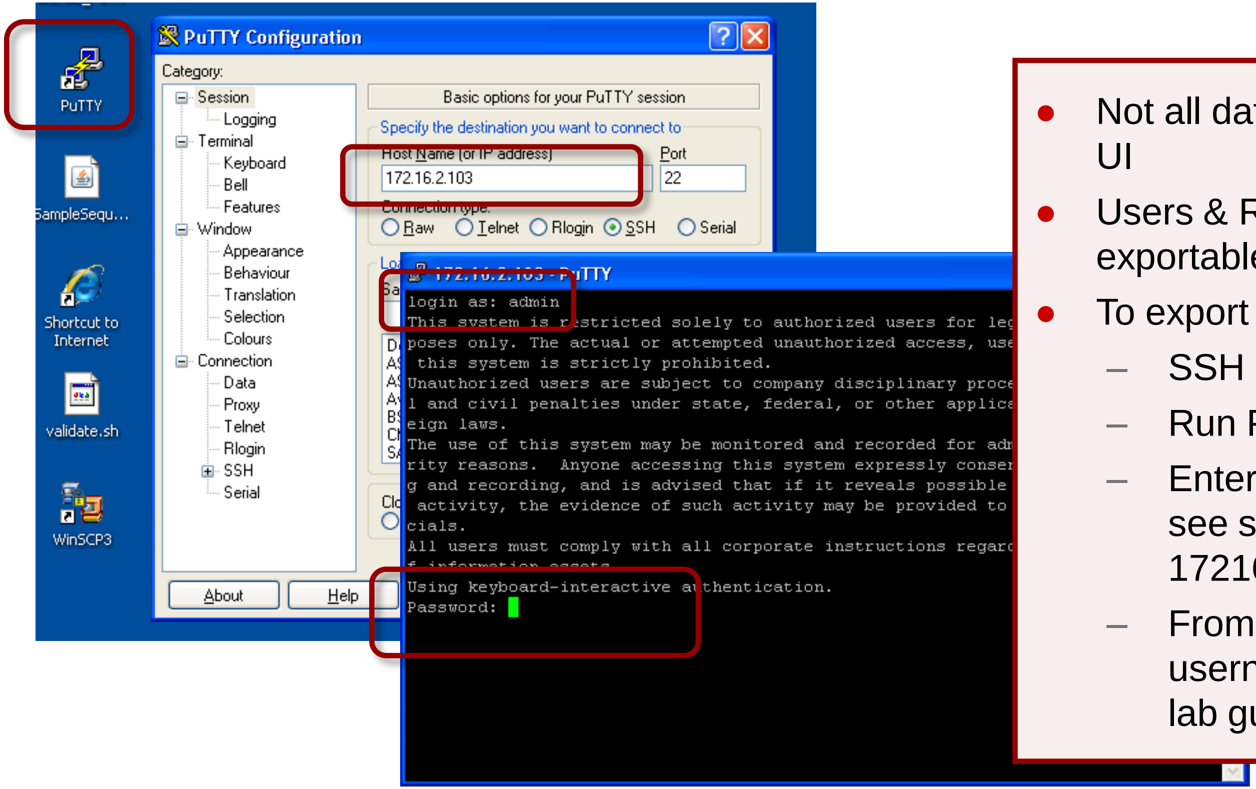
Student B



```
  <?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
- <sipentityFullTOList>
    <buildNumber>620103</buildNumber>
    <implementationVersion>6.2.0.0</implementat
    <specificationVersion>6.2</specificationVersio
  - <SipentityFullTO>
      <notes />
      <entitytype>ASM</entitytype>
      <fqdnoripaddr>172.16.2.105</fqdnoripaddr>
      <name>SM1</name>
      <cac_capable>false</cac_capable>
      <cdrSetting>none</cdrSetting>
      <credentialname />
      <do_monitoring>use-instance</do_monitori
      <monitor_proactive_secs>900</monitor_pro
```

Exporting SMGR Data from the Command Line – Needs SSH





PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 172.16.2.103

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

172.16.2.103 - PuTTY

```
login as: admin
This system is restricted solely to authorized users for leg
poses only. The actual or attempted unauthorized access, use
 this system is strictly prohibited.
Unauthorized users are subject to company disciplinary proce
l and civil penalties under state, federal, or other applica
eign laws.
The use of this system may be monitored and recorded for adm
rity reasons.  Anyone accessing this system expressly conse
g and recording, and is advised that if it reveals possible
 activity, the evidence of such activity may be provided to
cials.
All users must comply with all corporate instructions regarc
f information assets.
Using keyboard-interactive authentication.
Password:
```

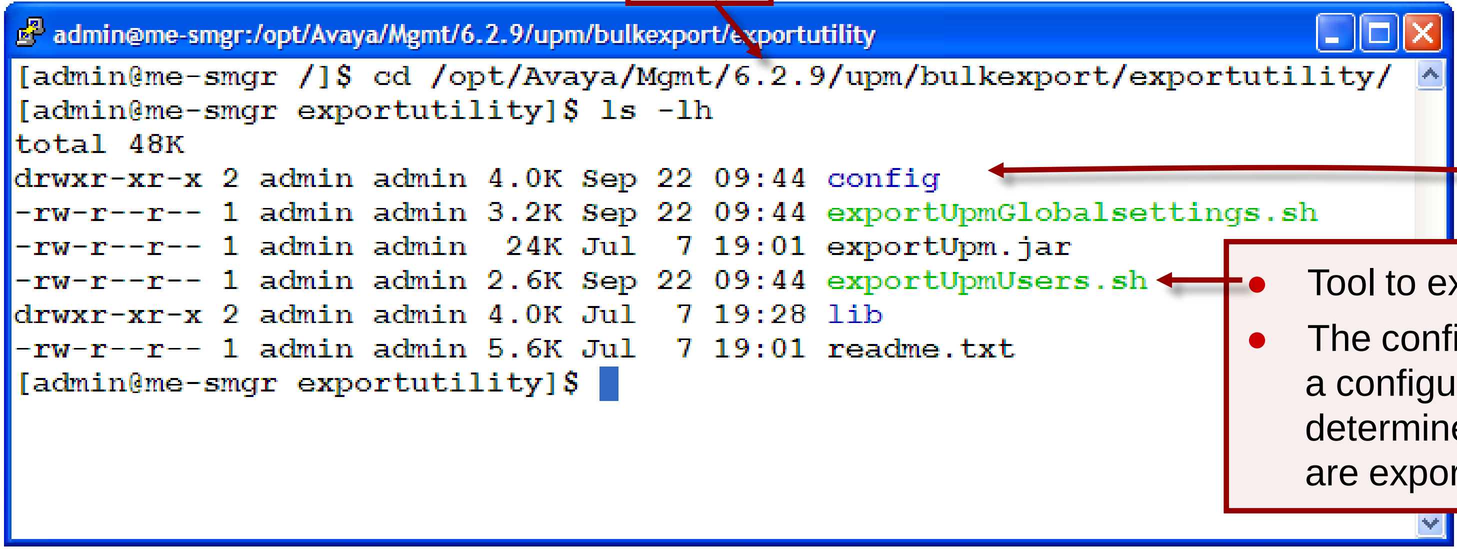
- Not all data is exportable from the SMGR UI
- Users & Roles are (currently) only exportable from the command line
- To export users and roles,
  - SSH into the SMGR server
  - Run Putty
  - Enter IP address of SMGR server – see student lab guide (eg 17216.2.103)
  - From the CLI console enter the SMGR username and password – see student lab guide (eg admin/admin)

Exporting SMGR Data – Export Utilities Location

Once logged in to SMGR with SSH, the export utilities are found at

- **/opt/Avaya/Mgmt/6.2.12/upm/bulkexport/exportutility**
  - Check release version – yours could be different

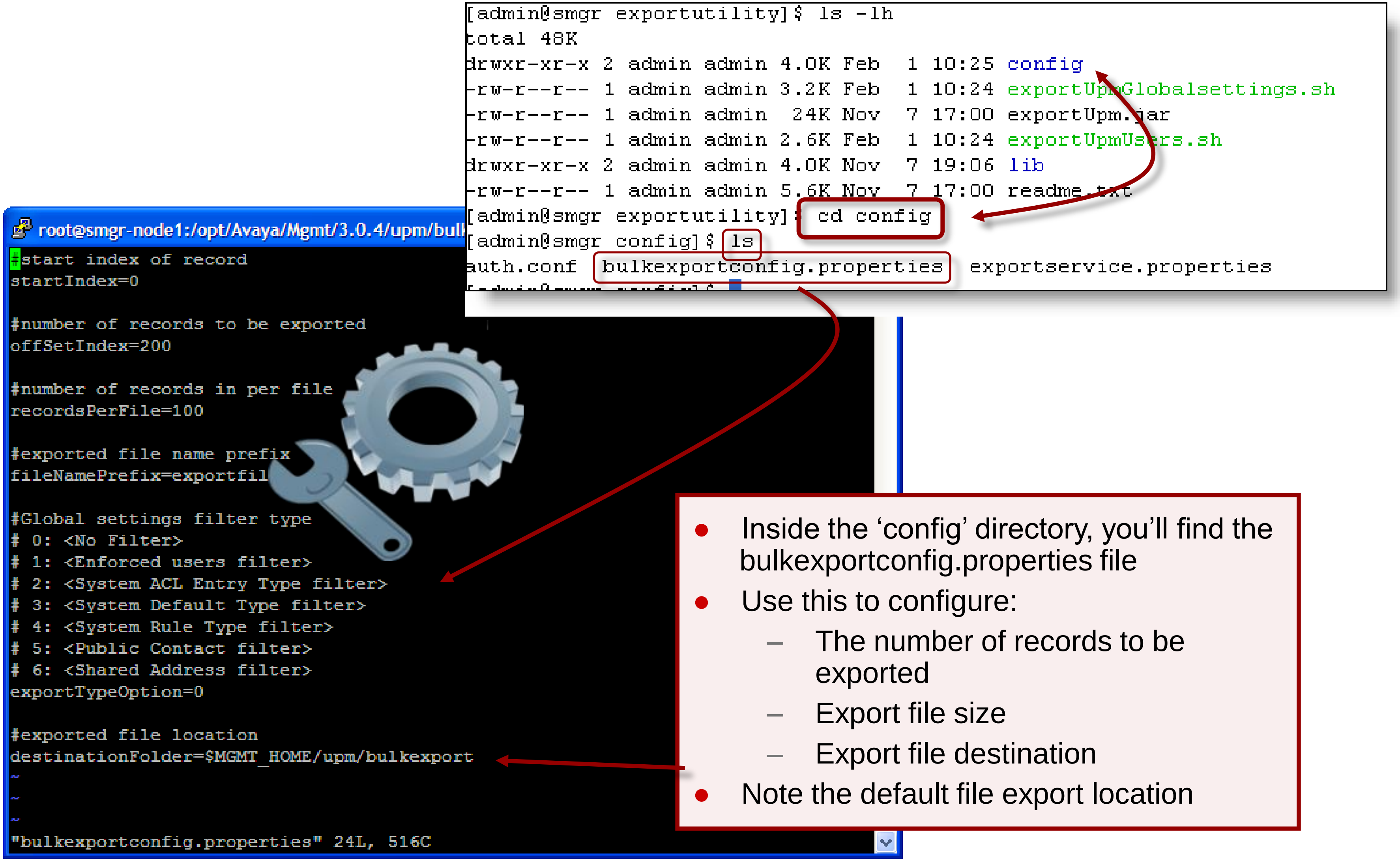
6.2.12


admin@me-smgr:/opt/Avaya/Mgmt/6.2.9/upm/bulkexport/exportutility

```
[admin@me-smgr /]$ cd /opt/Avaya/Mgmt/6.2.9/upm/bulkexport/exportutility/
[admin@me-smgr exportutility]$ ls -lh
total 48K
drwxr-xr-x 2 admin admin 4.0K Sep 22 09:44 config
-rw-r--r-- 1 admin admin 3.2K Sep 22 09:44 exportUpmGlobalsettings.sh
-rw-r--r-- 1 admin admin  24K Jul  7 19:01 exportUpm.jar
-rw-r--r-- 1 admin admin 2.6K Sep 22 09:44 exportUpmUsers.sh
drwxr-xr-x 2 admin admin 4.0K Jul  7 19:28 lib
-rw-r--r-- 1 admin admin 5.6K Jul  7 19:01 readme.txt
[admin@me-smgr exportutility]$
```

- Tool to export users
- The config directory contains a configuration tool that determines which records are exported

Exporting SMGR Data



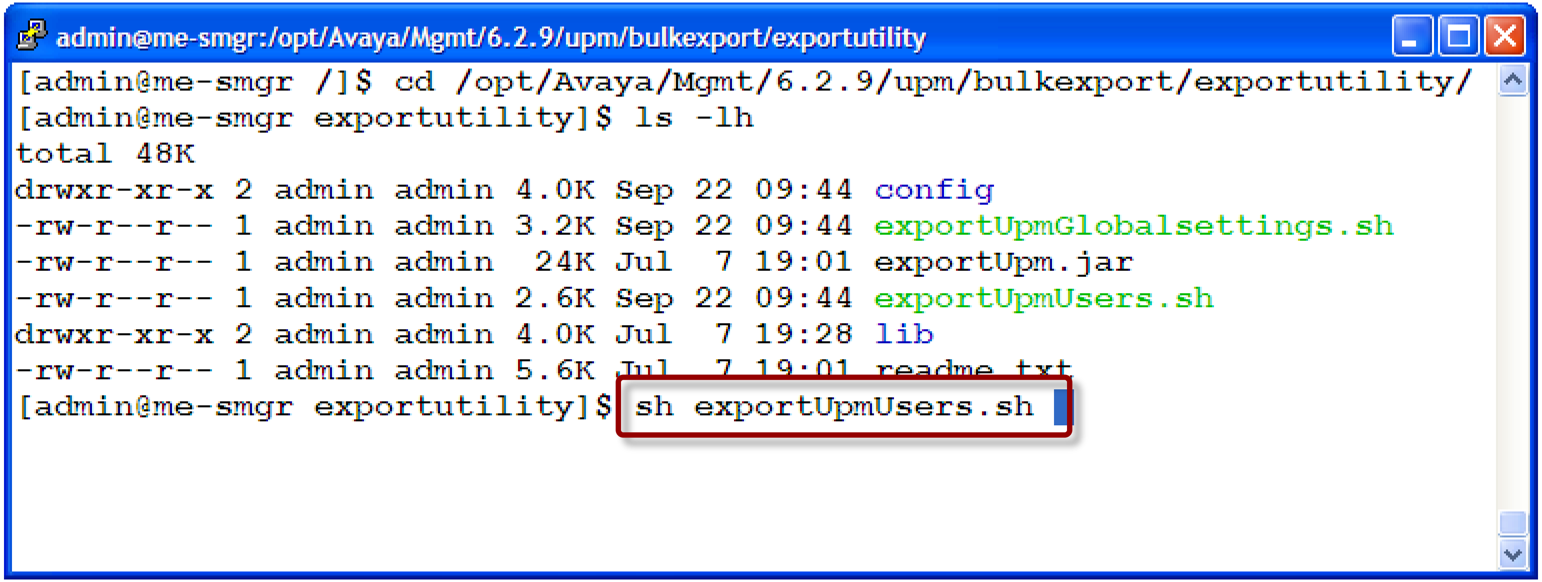
```
[admin@smgr exportutility]$ ls -lh
total 48K
drwxr-xr-x 2 admin admin 4.0K Feb  1 10:25 config
-rw-r--r-- 1 admin admin 3.2K Feb  1 10:24 exportUpmGlobalsettings.sh
-rw-r--r-- 1 admin admin  24K Nov  7 17:00 exportUpm.jar
-rw-r--r-- 1 admin admin 2.6K Feb  1 10:24 exportUpmUsers.sh
drwxr-xr-x 2 admin admin 4.0K Nov  7 19:06 lib
-rw-r--r-- 1 admin admin 5.6K Nov  7 17:00 readme.txt
[admin@smgr exportutility]$ cd config
[admin@smgr config]$ ls
auth.conf  bulkexportconfig.properties  exportservice.properties
```

root@smgr-node1:/opt/Avaya/Mgmt/3.0.4/upm/bul

```
#start index of record
startIndex=0

#number of records to be exported
offSetIndex=200

#number of records in per file
recordsPerFile=100

#exported file name prefix
fileNamePrefix=exportfil

#Global settings filter type
# 0: <No Filter>
# 1: <Enforced users filter>
# 2: <System ACL Entry Type filter>
# 3: <System Default Type filter>
# 4: <System Rule Type filter>
# 5: <Public Contact filter>
# 6: <Shared Address filter>
exportTypeOption=0

#exported file location
destinationFolder=$MGMT_HOME/upm/bulkexport
~
~
~
"bulkexportconfig.properties" 24L, 516C
```

- Inside the ‘config’ directory, you’ll find the bulkexportconfig.properties file
- Use this to configure:
  - The number of records to be exported
  - Export file size
  - Export file destination
- Note the default file export location

Exporting SMGR Data – sh exportUpmUsers.sh


admin@me-smgr:/opt/Avaya/Mgmt/6.2.9/upm/bulkexport/exportutility

```
[admin@me-smgr /]$ cd /opt/Avaya/Mgmt/6.2.9/upm/bulkexport/exportutility/
[admin@me-smgr exportutility]$ ls -lh
total 48K
drwxr-xr-x 2 admin admin 4.0K Sep 22 09:44 config
-rw-r--r-- 1 admin admin 3.2K Sep 22 09:44 exportUpmGlobalsettings.sh
-rw-r--r-- 1 admin admin  24K Jul  7 19:01 exportUpm.jar
-rw-r--r-- 1 admin admin 2.6K Sep 22 09:44 exportUpmUsers.sh
drwxr-xr-x 2 admin admin 4.0K Jul  7 19:28 lib
-rw-r--r-- 1 admin admin 5.6K Jul  7 19:01 readme.txt
[admin@me-smgr exportutility]$ sh exportUpmUsers.sh
```

- Command to export users shown above
- Can override defaults (in bulkexportconfig.properties) using optional

- f : Export file name prefix
- r : Records per file
- d : Destination Folder
- s : Record starting index
- e : End offset index (number of records)

E.g

```
$ sh exportUpmUsers.sh -f name -s 10
```

Exercise: Export User Data using CLI Utilities

Objective & Outcome

The objective of this exercise is to learn to use SMGR's CLI utilities to export data. By the time you are done, you will have SSH'd in to SMGR, triggered the export of data, and will have an exported data file ready for inspection.

1. SSH in to SMGR
   - Run Putty from the student desktop.
   - Enter IP address of SMGR server **172.16.x.103**
   - From the CLI console enter the SMGR username: **admin** password **admin**

2. Navigate to export utilities
   - type: **cd /opt/Avaya/Mgmt/6.2.12/upm/bulkexport/exportutility**

3. Run the export shell
   - type: **sh exportUpmUsers.sh**

   SMGR will take a few moments to export the file

4. Check the exported file
   - Navigate to the export directory.

   type: **cd /opt/Avaya/Mgmt/6.2.12/upm/bulkexport/**
   - check for file with name something like 'exportfile_133043382932.zip'

Team Activity
Student B to drive,
with student A
shadowing

Student A

Student B

CLI Exporting SMGR Data – Scheduling

- You can also schedule an export to be performed

- t : Set export scheduled time

YYYY:MM:DD:HH:MM:SS

- E.g:

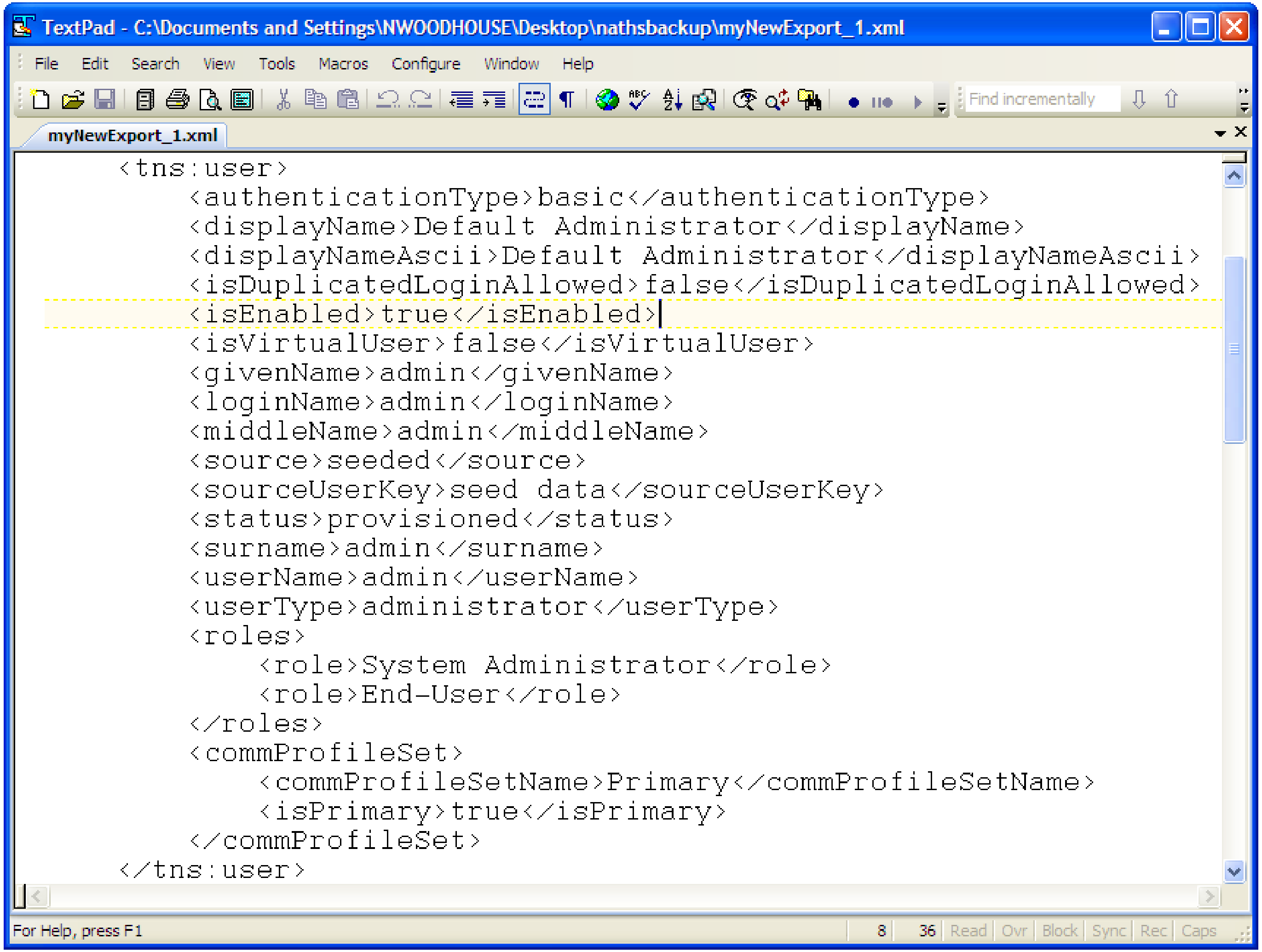
exportUpmUsers.sh –t 010:05:01:12:00:00

???

1st of May 2010, at Midday

Script regular
data exports?

CLI Exporting SMGR Data



TextPad - C:\Documents and Settings\NWOODHOUSE\Desktop\nathsbackup\myNewExport_1.xml
File Edit Search View Tools Macros Configure Window Help
Find incrementally
myNewExport_1.xml
For Help, press F1
8 36 Read Ovr Block Sync Rec Caps

```
    <tns:user>
        <authenticationType>basic</authenticationType>
        <displayName>Default Administrator</displayName>
        <displayNameAscii>Default Administrator</displayNameAscii>
        <isDuplicatedLoginAllowed>false</isDuplicatedLoginAllowed>
        <isEnabled>true</isEnabled>
        <isVirtualUser>false</isVirtualUser>
        <givenName>admin</givenName>
        <loginName>admin</loginName>
        <middleName>admin</middleName>
        <source>seeded</source>
        <sourceUserKey>seed data</sourceUserKey>
        <status>provisioned</status>
        <surname>admin</surname>
        <userName>admin</userName>
        <userType>administrator</userType>
        <roles>
            <role>System Administrator</role>
            <role>End-User</role>
        </roles>
        <commProfileSet>
            <commProfileSetName>Primary</commProfileSetName>
            <isPrimary>true</isPrimary>
        </commProfileSet>
    </tns:user>
```

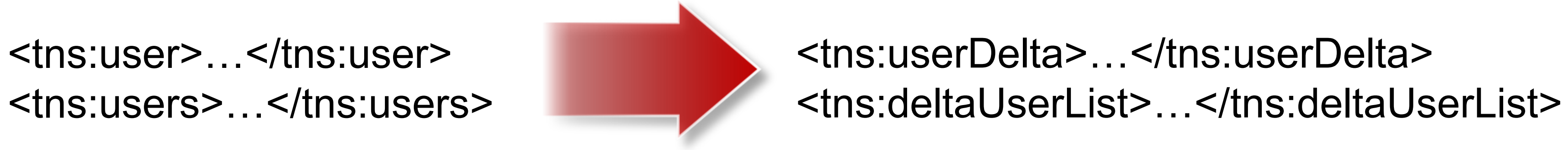
- Data exported from the command line can be imported through the GUI.

Export XML Format

- XML File can be amended for use in ‘partial’ import

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:ns3="http://xml.avaya.com/schema/import_csm_mm"
xmlns:ns4="http://xml.avaya.com/schema/import_csm_cm"
xmlns:ns5="http://xml.avaya.com/schema/import_sessionmanager"
xmlns:ns6="http://xml.avaya.com/schema/deltaImport"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">
```

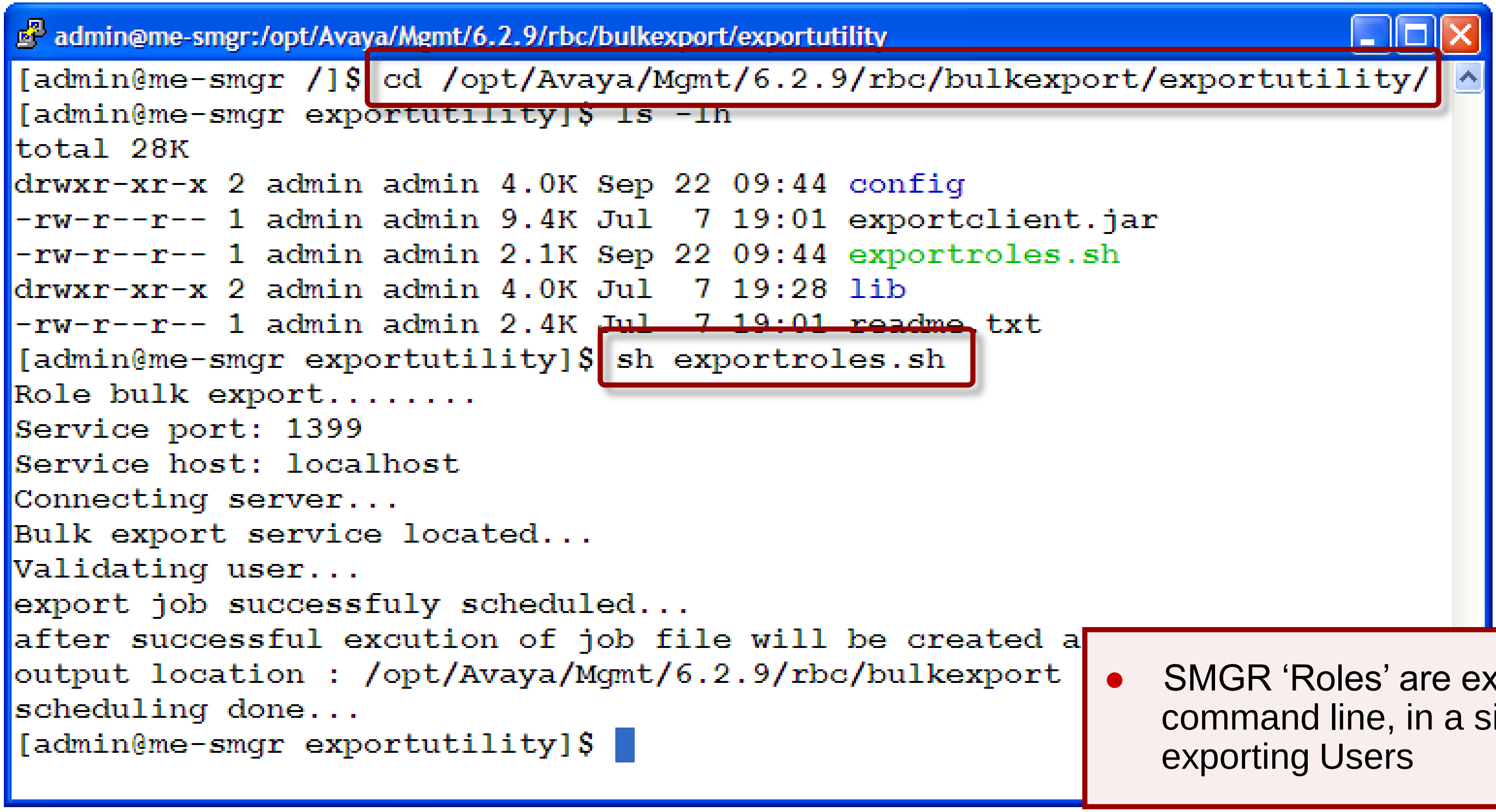
```
<tns:deltaUserList xmlns:ns3=http://xml.avaya.com/schema/import1
xmlns:tns="http://xml.avaya.com/schema/deltaImport"
xmlns:xsi="http://www.w3.org/2001/XMLSchema instance"
xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport userdeltaimport.xsd ">
```



```
<tns:user>…</tns:user>
<tns:users>…</tns:users>
```

```
<tns:userDelta>…</tns:userDelta>
<tns:deltaUserList>…</tns:deltaUserList>
```

Separate CLI for Exporting Roles



admin@me-smgr:/opt/Avaya/Mgmt/6.2.9/rbc/bulkexport/exportutility

```
[admin@me-smgr /]$ cd /opt/Avaya/Mgmt/6.2.9/rbc/bulkexport/exportutility/
[admin@me-smgr exportutility]$ ls -lh
total 28K
drwxr-xr-x 2 admin admin 4.0K Sep 22 09:44 config
-rw-r--r-- 1 admin admin 9.4K Jul  7 19:01 exportclient.jar
-rw-r--r-- 1 admin admin 2.1K Sep 22 09:44 exportroles.sh
drwxr-xr-x 2 admin admin 4.0K Jul  7 19:28 lib
-rw-r--r-- 1 admin admin 2.4K Jul  7 19:01 readme.txt
[admin@me-smgr exportutility]$ sh exportroles.sh
Role bulk export........
Service port: 1399
Service host: localhost
Connecting server...
Bulk export service located...
Validating user...
export job successfuly scheduled...
after successful excution of job file will be created a
output location : /opt/Avaya/Mgmt/6.2.9/rbc/bulkexport
scheduling done...
[admin@me-smgr exportutility]$
```

- SMGR ‘Roles’ are exported via the command line, in a similar way to exporting Users

AVAYA | LEARNING

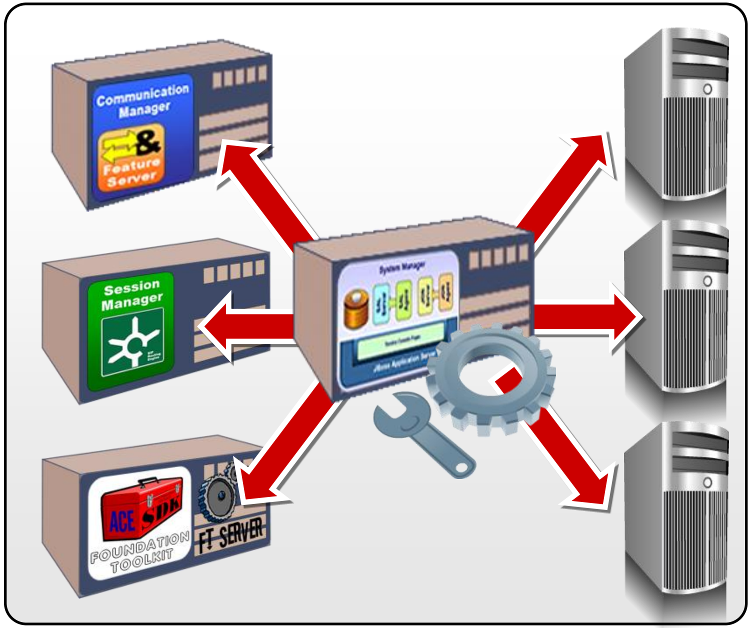
Module 06: SMGR & Business Continuity

Lesson 01: Backing Up SMGR Data

Lesson Duration: 30 Minutes

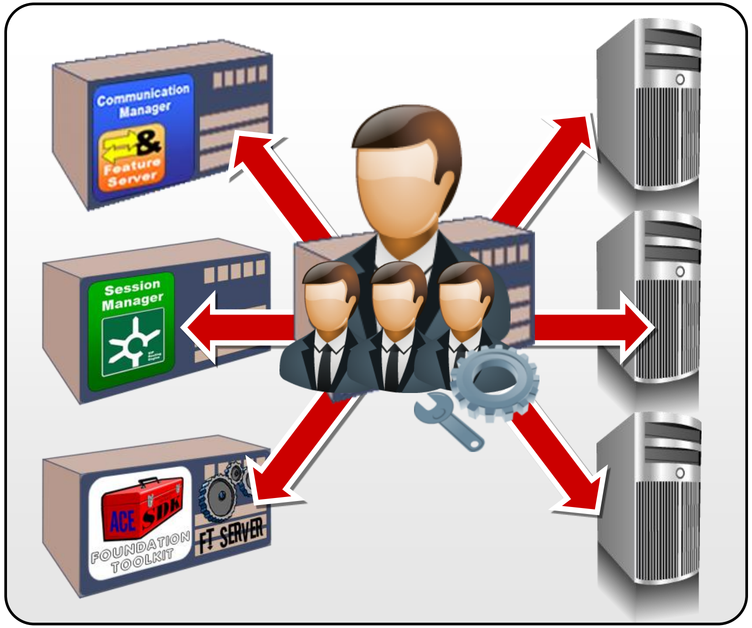
Critical Information Held by Avaya Aura® SMGR

- **Product Management Data**



- Element definitions
- Configuration
- Routing Policies, endpoint profiles

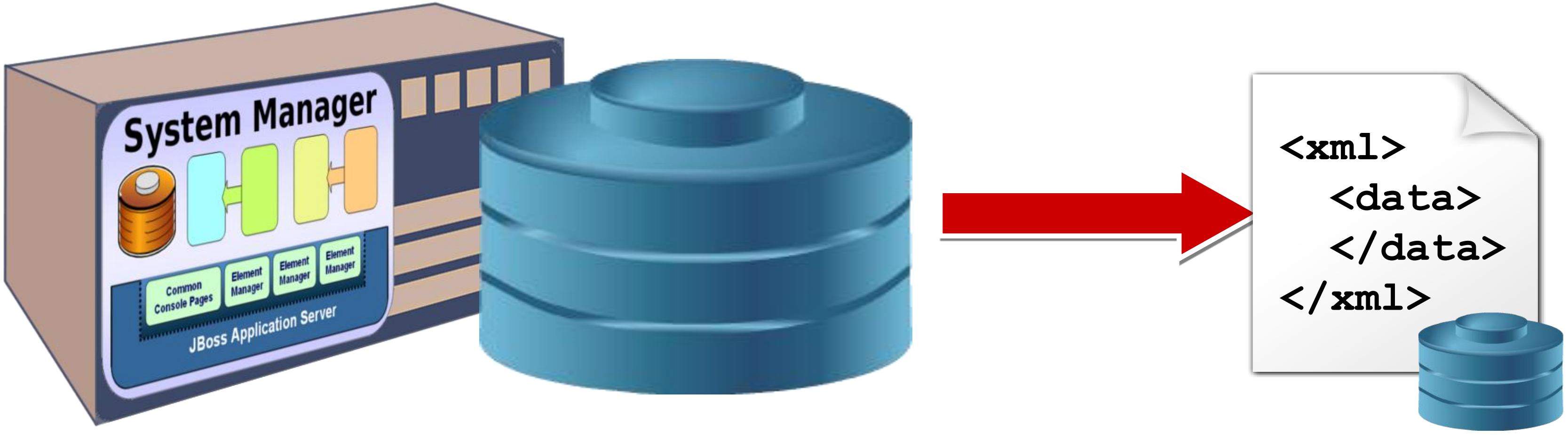
- **User Profile Data**
  - Admin & communication users



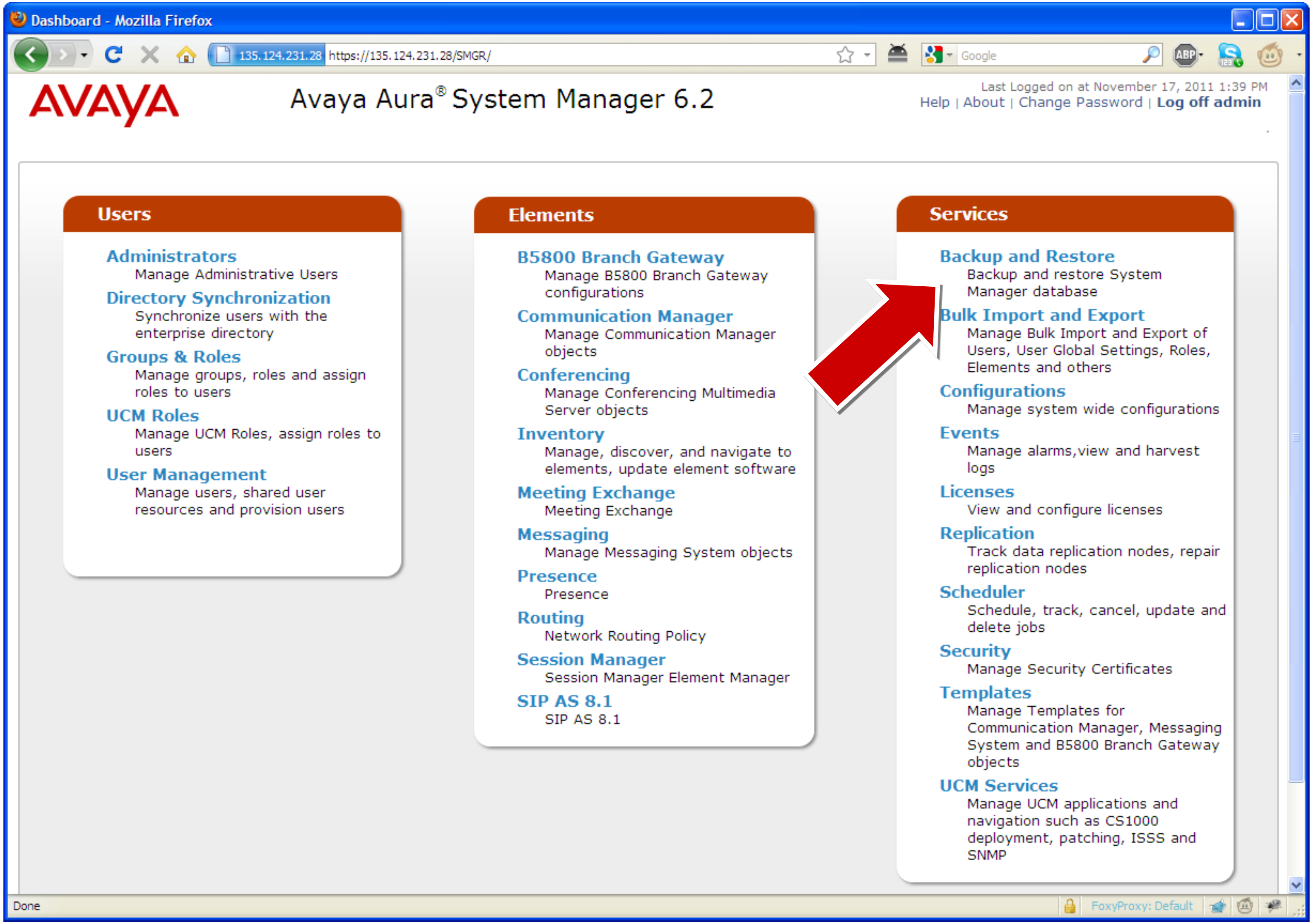
- User profiles, adresses, roles etc.
- Communication profiles
- Application sequencing

Lesson Duration: 30 Minutes

Backing Up SMGR Data



Backing Up SMGR Data (continued)



Dashboard - Mozilla Firefox
135.124.231.28 https://135.124.231.28/SMGR/
Google

Avaya Aura® System Manager 6.2

Last Logged on at November 17, 2011 1:39 PM

Help | About | Change Password | Log off admin

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

UCM Roles
Manage UCM Roles, assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway configurations

Communication Manager
Manage Communication Manager objects

Conferencing
Manage Conferencing Multimedia Server objects

Inventory
Manage, discover, and navigate to elements, update element software

Meeting Exchange
Meeting Exchange

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

Scheduler
Schedule, track, cancel, update and delete jobs

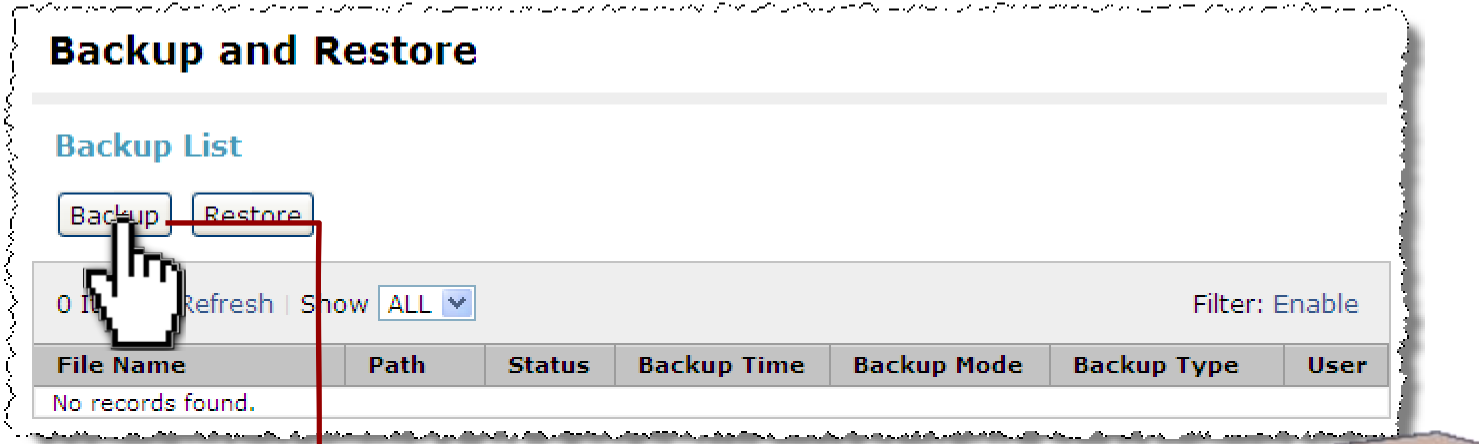
Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway objects

UCM Services
Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

Backing Up SMGR Data – 2 Options: to Local Drive

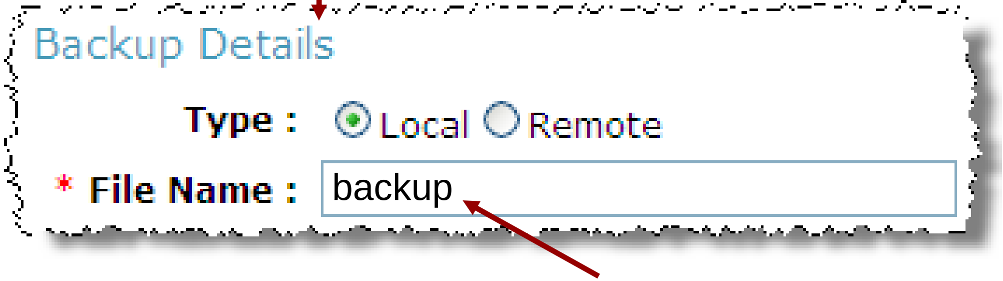
- A backup can be created on the local file system.



Backup and Restore

Backup List

File Name	Path	Status	Backup Time	Backup Mode	Backup Type	User
No records found.						



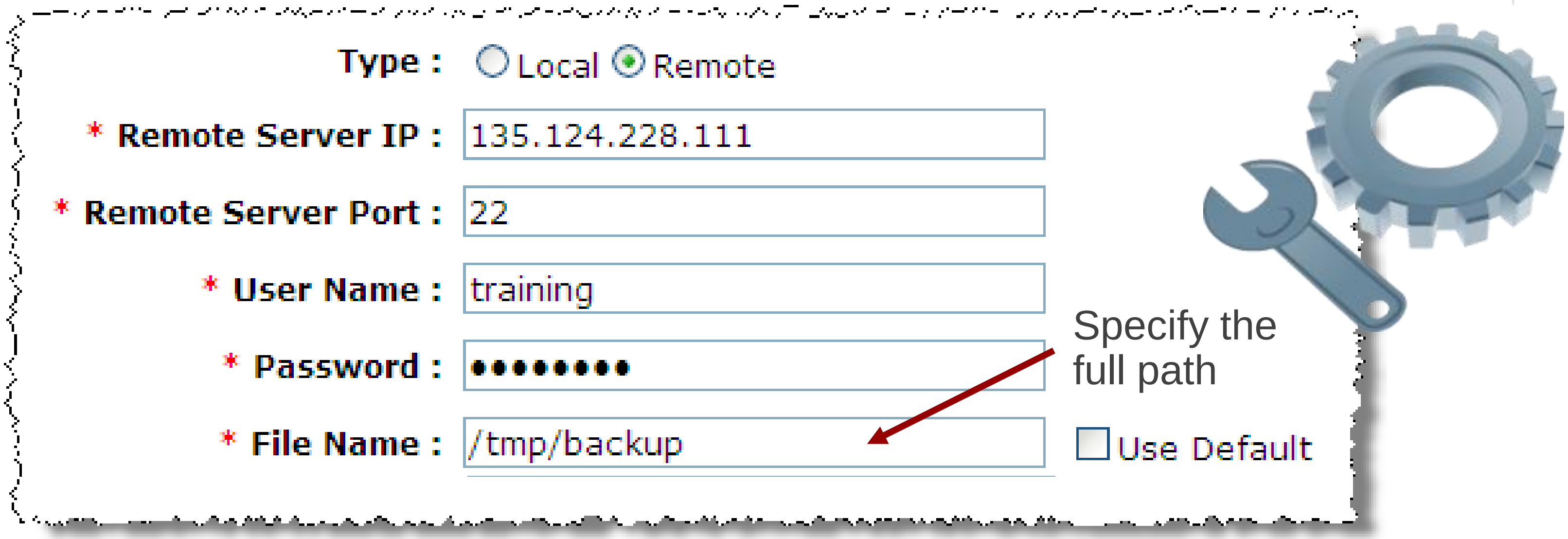
Backup Details

Type : ● Local ○ Remote

* File Name : backup

Only specify the filename, not the path

Backing Up SMGR Data – 2 Options: to Remote Server



Type :	○ Local ● Remote
* Remote Server IP :	135.124.228.111
* Remote Server Port :	22
* User Name :	training
* Password :	●●●●●●●●●
* File Name :	/tmp/backup

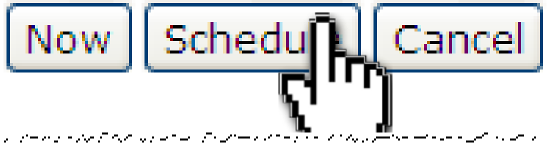
□ Use Default

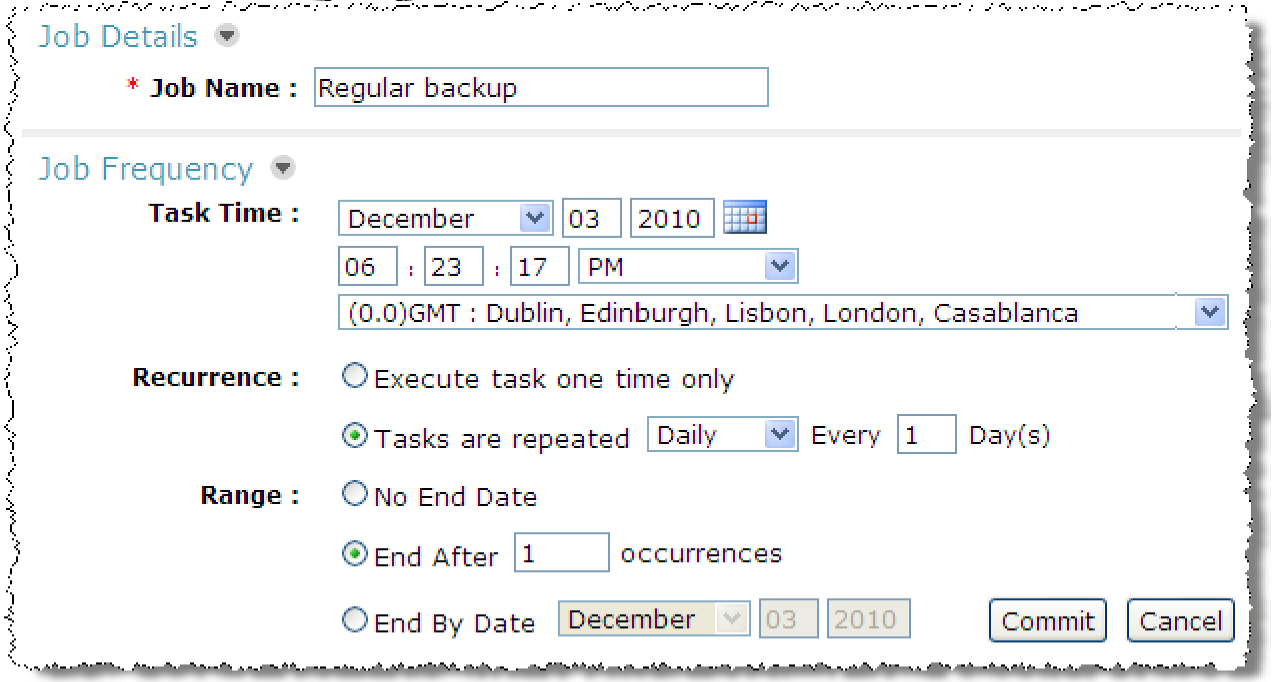
Specify the full path

- SMGR data can also be backup to a remote Linux server (safer).
- When backi remote server you will need the remote s in etail

Backing Up SMGR Data – Scheduling

- Can be performed immediately (‘now’)
- Can be scheduled to take in the future
- Scheduled backups can be recurring – *Every Wednesday at 11pm*





Job Details

* Job Name : Regular backup

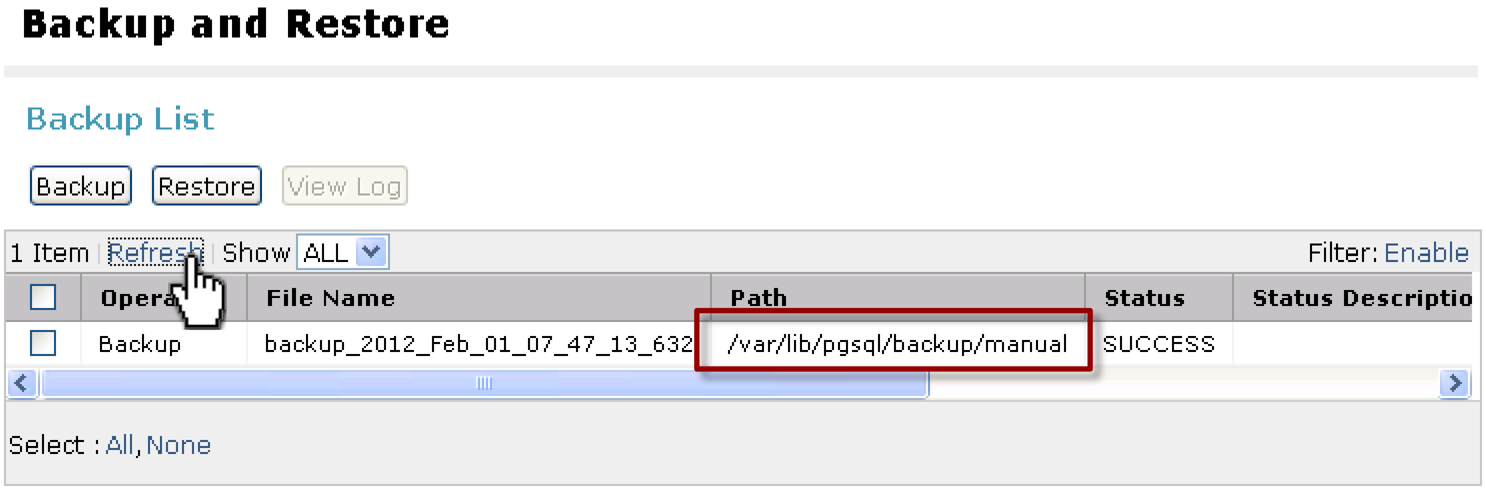
Job Frequency

Task Time : December 03 2010
06 : 23 : 17 PM
(0.0)GMT : Dublin, Edinburgh, Lisbon, London, Casablanca

Recurrence : ○ Execute task one time only
● Tasks are repeated Daily Every 1 Day(s)

Range : ○ No End Date
● End After 1 occurrences
○ End By Date December 03 2010

Backing Up SMGR Data – Locating Backup



Backup and Restore

Backup List

1 Item | Refresh | Show ALL   Filter: Enable

□	Opera	File Name	Path	Status	Status Descriptio
□	Backup	backup_2012_Feb_01_07_47_13_632	/var/lib/pgsql/backup/manual	SUCCESS	

Select : All, None

- You may need to click the ‘refresh’ button while the status is ‘RUNNING’
- When the backup completes, SMGR will summarize the path & filename

To view the backup, SSH into SMGR machine.
The default local location is /var/lib/pgsql/backup/manual

Exercise: Perform a Local Back Up of All SMGR Data

Objective & Outcome

The objective is to learn how to backup SMGR data locally.

1. Navigate to Home > Services > Backup and Restore >. Click ‘Backup’
2. Select backup type: ***Local***. Enter name for back up file E.g. ‘**smgrdata**’

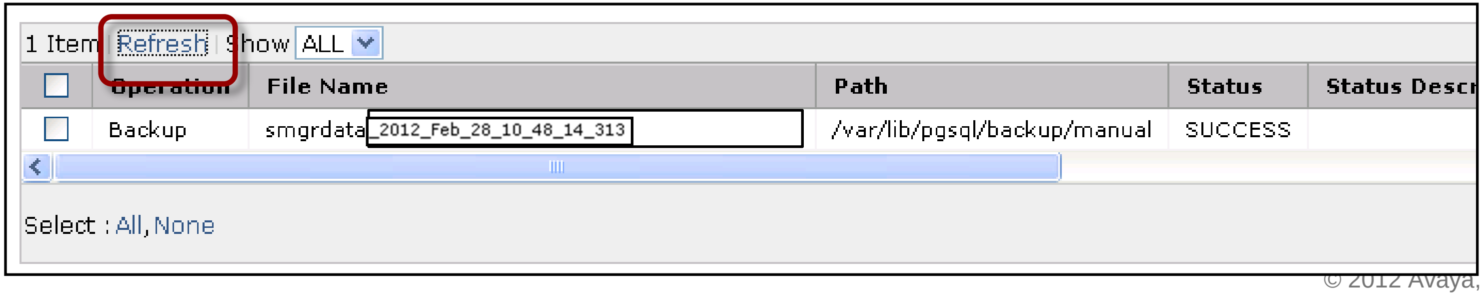
   The file will automatically be appended with today’s date.
3. Periodically click Refresh. Check that the backup is successful
4. SSH in to the server and navigate to the backup file. Take a look at contents of backup ZIP!

   ```
   # cd  /var/lib/pgsql/backup/manual.
   # unzip backup*.zip
   # ls –lh;
   # cat <filename>
   ```
5. If time permits, go through the steps of scheduling a maintenance back up tonight at midnight

Team Activity
Student A to drive,
with student B
shadowing

Student A

Student B



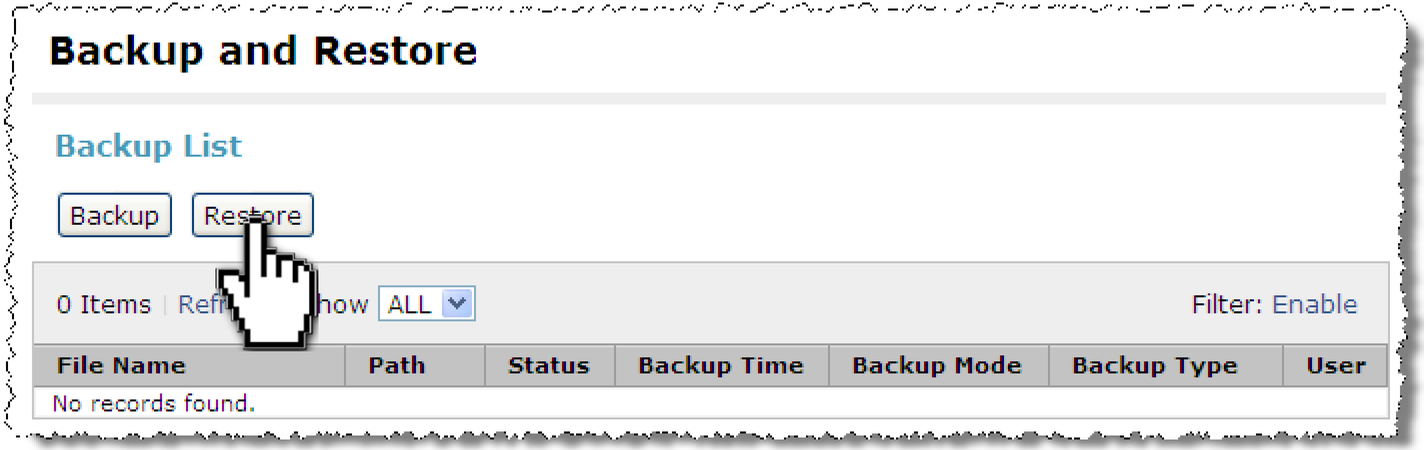
1 Item | Refresh | Show ALL

□	Operation	File Name	Path	Status	Status Descr
□	Backup	smgrdata_2012_Feb_28_10_48_14_313	/var/lib/pgsql/backup/manual	SUCCESS	

Select : All, None

Restoring From Backup

- When needed, you can restore SMGR data from backup.



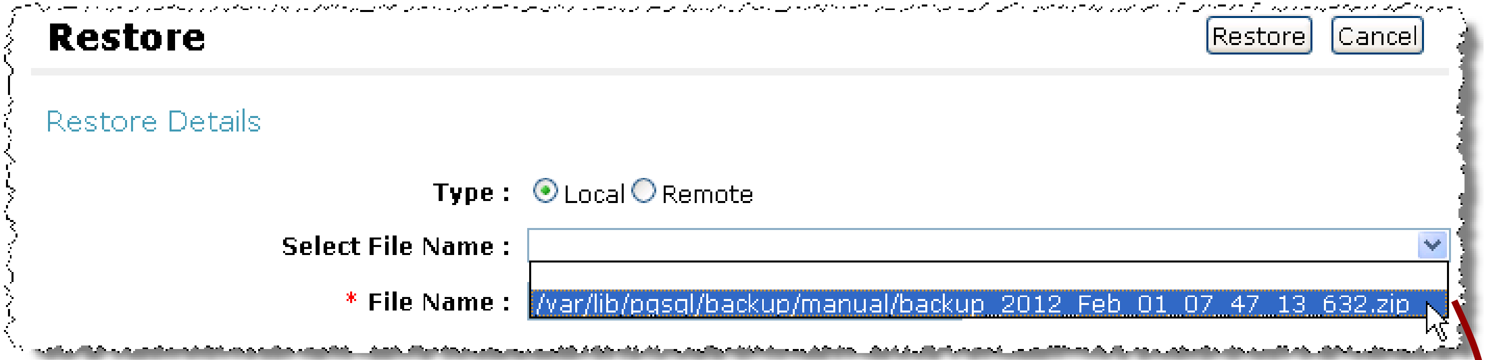
Backup and Restore

Backup List

0 Items | Refresh | Show ALL

Filter: Enable

File Name	Path	Status	Backup Time	Backup Mode	Backup Type	User
No records found.						



Restore

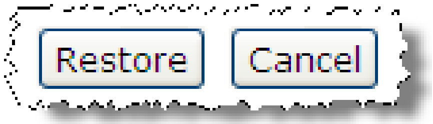
Restore Details

Type : ● Local ○ Remote

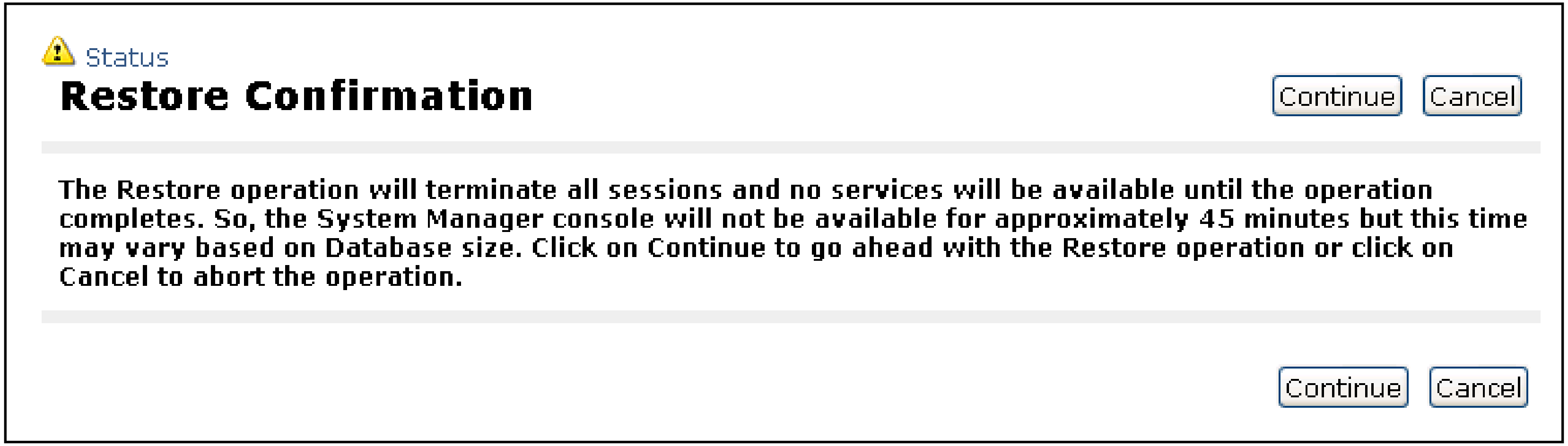
Select File Name : /var/lib/pgsql/backup/manual/backup_2012_Feb_01_07_47_13_632.zip

* File Name :

SMGR will remember previous backups



Restoring From Backup (continued)



Restore Confirmation

The Restore operation will terminate all sessions and no services will be available until the operation completes. So, the System Manager console will not be available for approximately 45 minutes but this time may vary based on Database size. Click on Continue to go ahead with the Restore operation or click on Cancel to abort the operation.

- Be warned that this is a dangerous operation!
- It will wipe existing configuration in favor of the settings found in the backup.
- Can take a long time to complete
  - Up to 45 minutes (depending on data)

Exercise: Restoring from Backup

Objective & Outcome

The objective of this exercise is to learn how to restore SMGR to a previous data set. You will first delete some settings, but, following data restore, the deleted settings will be restored.

1. **Delete some SMGR data**
   - go to Home > Users > User Management > Manage Users. Delete some users
   - go to Home > Elements > Routing > SIP Entities. Delete some SIP Entities
2. **Restore from Backup**
   - go to Home > Services > Backup and Restore. Click ‘Restore’
   - Select Type: ***Local***.
   - From the drop down list, select the backup file to restore
   - Click ‘***Restore***’

The restoration may take around 15 minutes

3. **Check restored data**
   - go to Home > Users > User Management > Manage Users. Check deleted users are restored
   - go to Home > Elements > Routing > SIP Entities. Check deleted SIP Entities are restored

Team Activity
Student B to drive,
with student A
shadowing

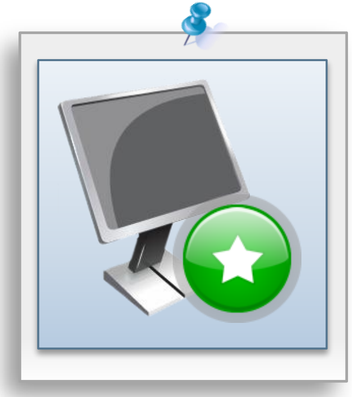
Student A

Student B

Exercise: Perform a Remote Back Up of SMGR Data

Objective & Outcome
The objective of this exercise is to learn how to perform a remote backup of SMGR data. By the time you are done, your SMGR data will be backed up to the SMGR server of another student team in your group.

1. Organise team pairing: Pod 1 & 2, Pod 3 & 4, Pod 5 & 6
2. Navigate to Home > Services > Backup and Restore >. Click 'Backup'
3. Select backup type: ***Remote***.
   - Enter IP address, username and password for remote server (see student lab guide.)
   - Choose name for back up file E.g. **smgrdataPodx**
   - Click '***Now***'
4. Periodically click Refresh. Check that the backup is successful
5. SSH in to the other server and navigate to the backup file.
   - # **cd /var/lib/pgsql/backup/manual.**



Team Activity
Student A to drive,
with student B
shadowing

Student A

Student B

AVAYA

INTELLIGENT COMMUNICATIONS

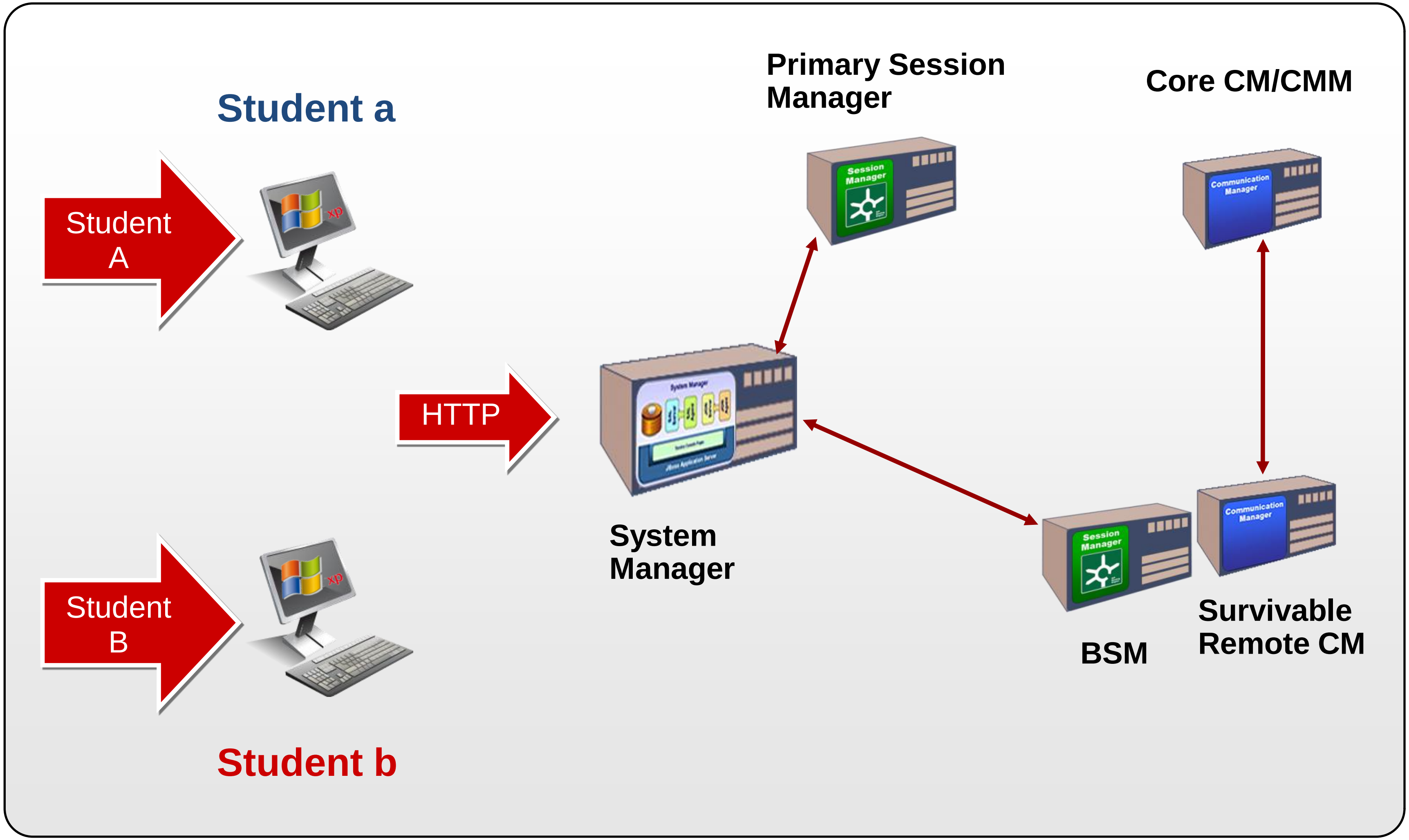
5U00096V Version 1.0

Session Manager Administration 6.2

Please note that this course does not have audio. Click the forward/backward arrows to navigate this course.

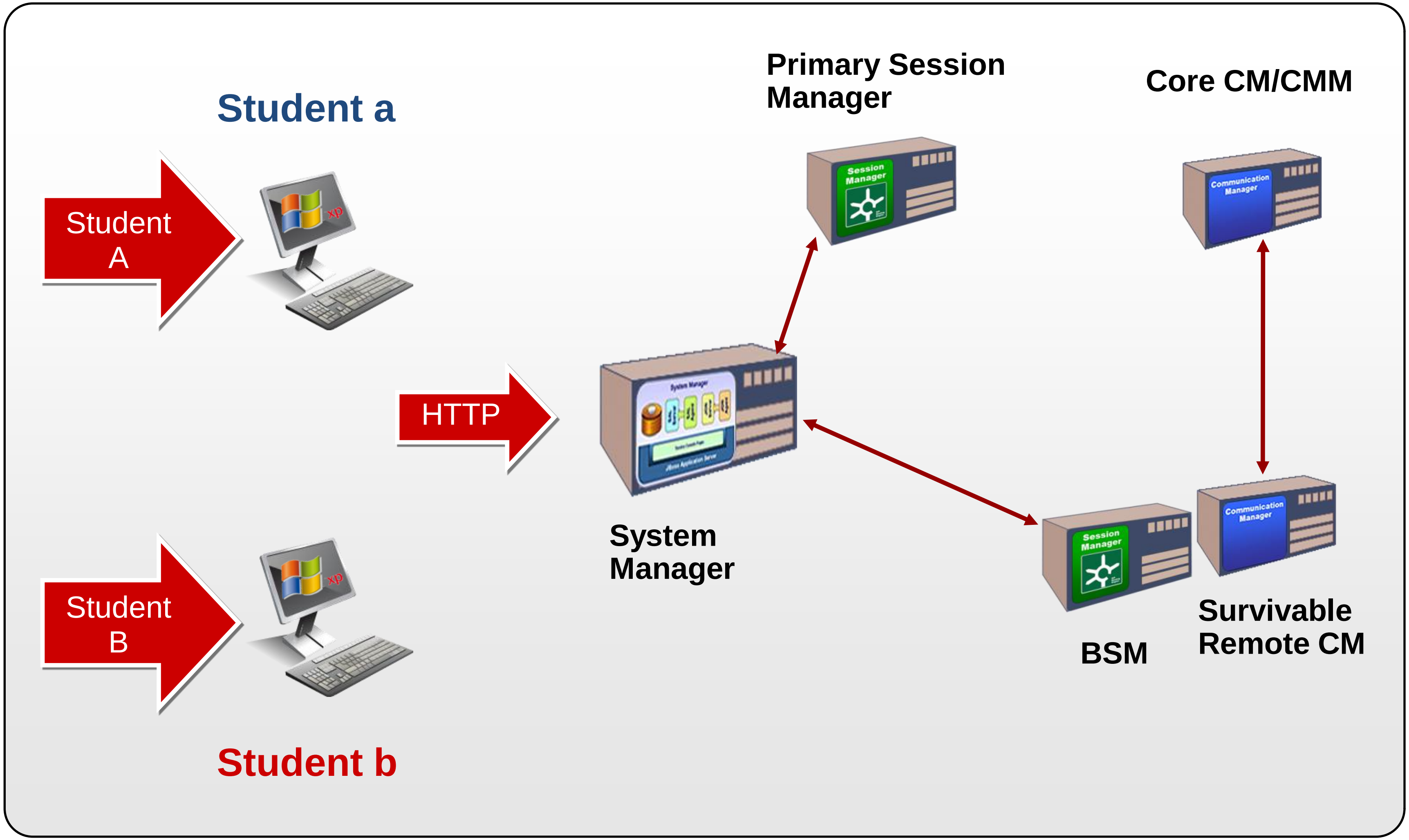
Classroom Layout

Pod 1 – 172.16.1.x



Classroom Layout (continued)

Pod 2 – 172.16.2.x



Student a

Student A

Student B

Student b

HTTP

Primary Session Manager

Core CM/CMM

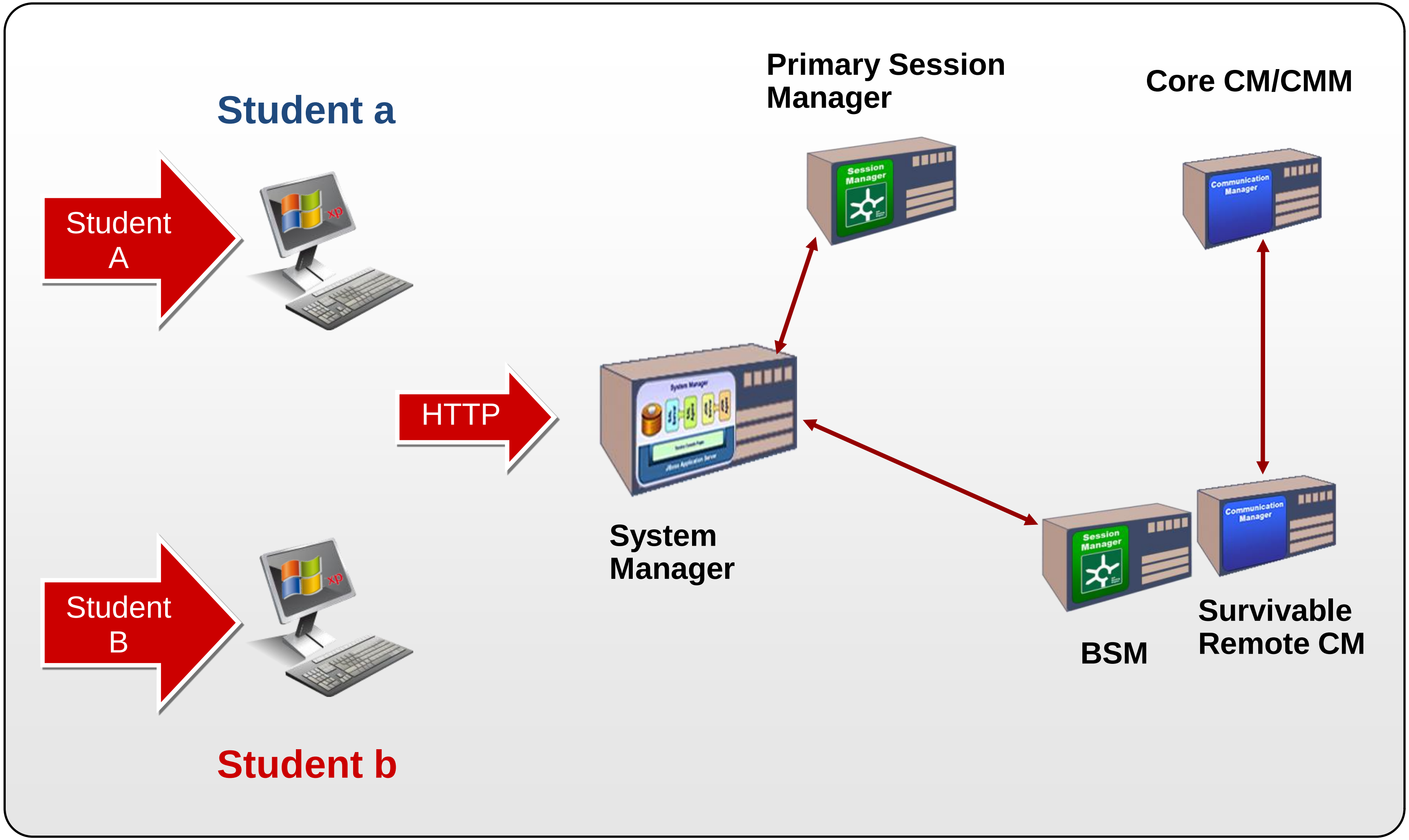
System Manager

BSM

Survivable Remote CM

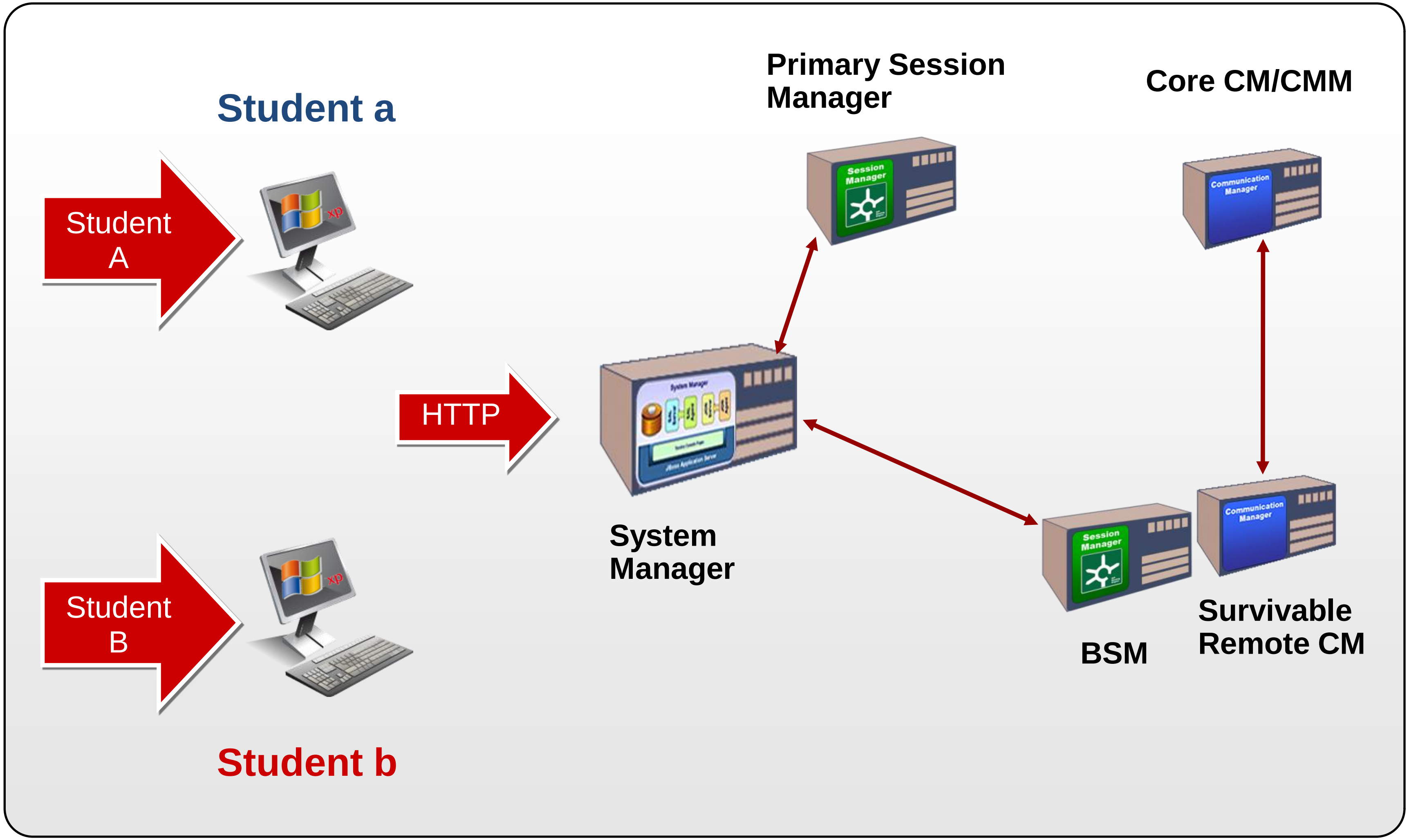
Classroom Layout (continued)

Pod 3 – 172.16.3.x



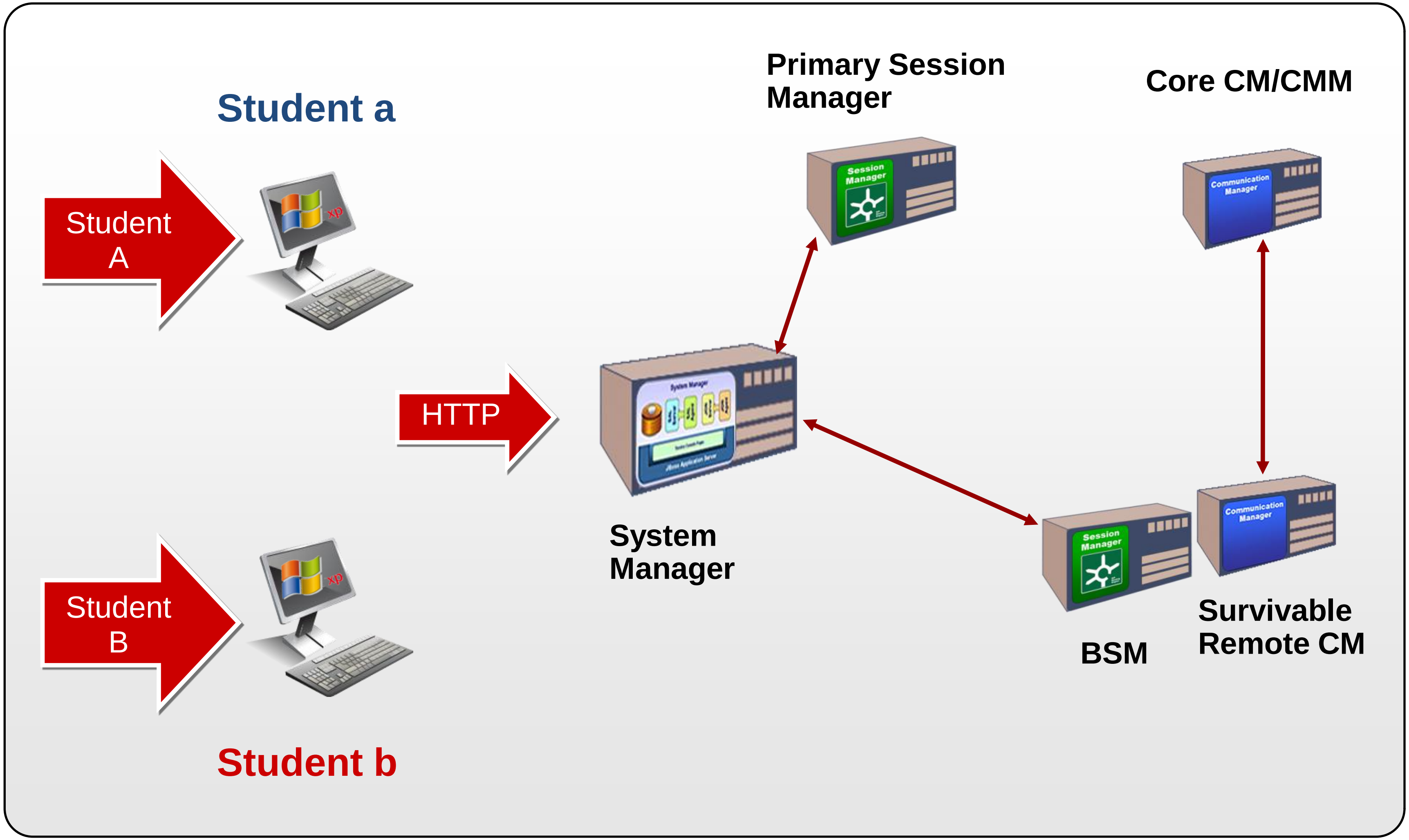
Classroom Layout (continued)

Pod 4 – 172.16.4.x



Classroom Layout (continued)

Pod 5 – 172.16.5.x



Student a

Student A

Student B

Student b

HTTP

Primary Session Manager

Core CM/CMM

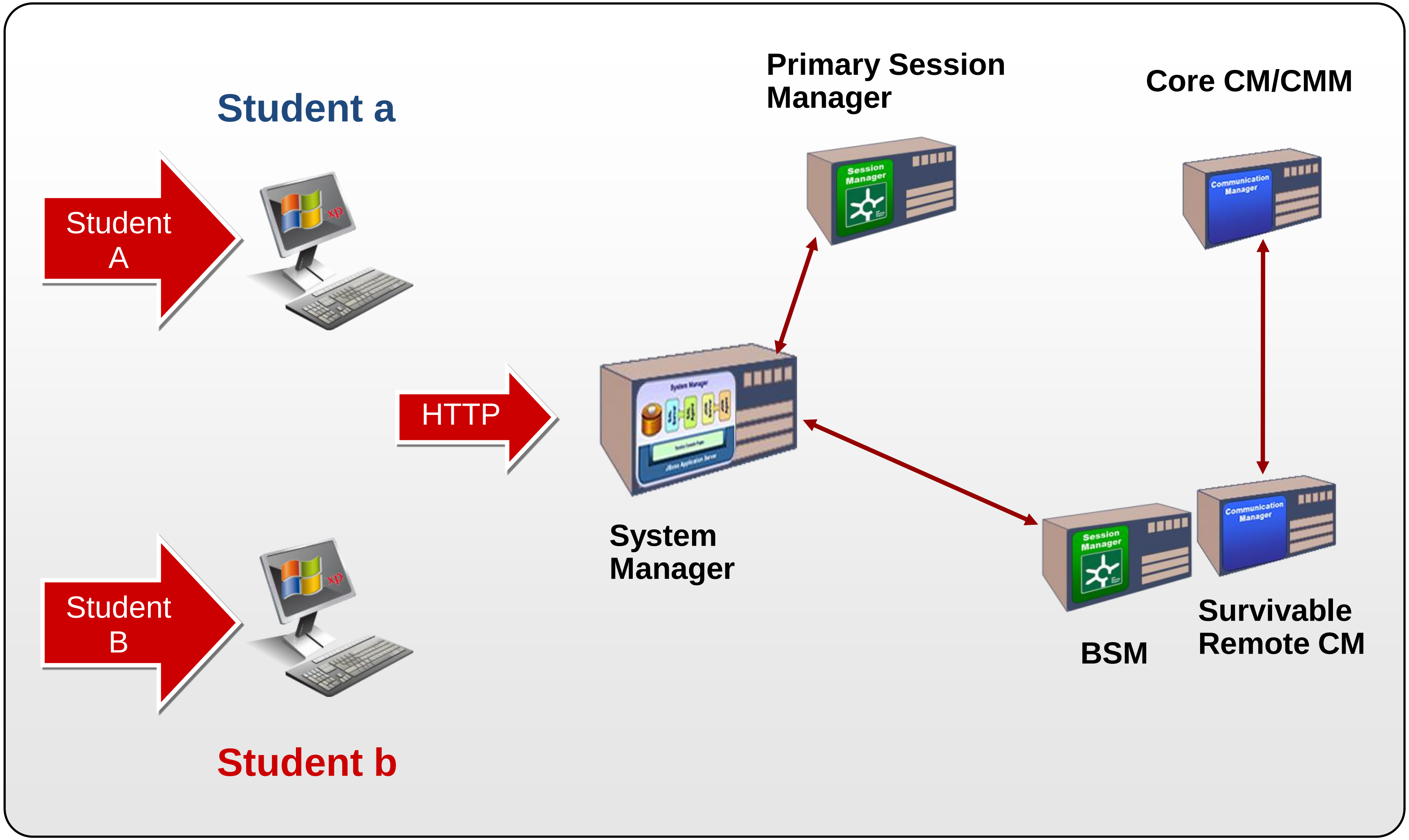
System Manager

BSM

Survivable Remote CM

Classroom Layout (continued)

Pod 6 – 172.16.6.x



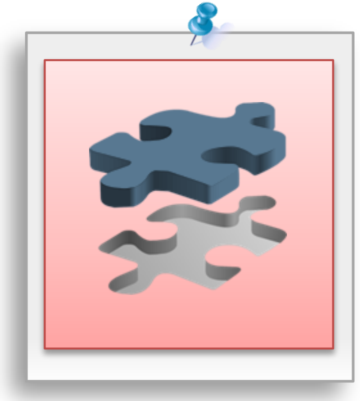
Lesson 01

Introducing Session Manager

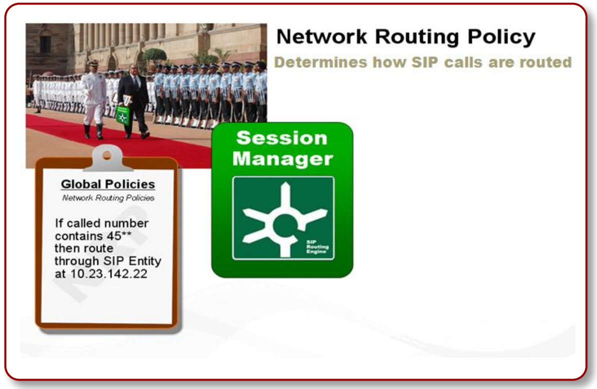
Lesson Objective

After completing this lesson, you will be able to:

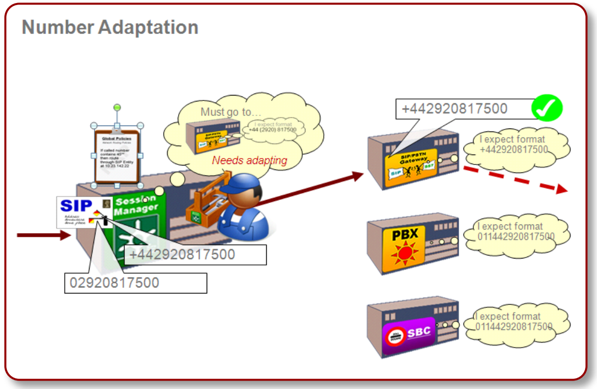
- Understand the purpose and function of Session Manager.



Session Manager Overview


Network Routing Policy
Determines how SIP calls are routed
Session Manager
Global Policies
Network Routing Policies
If called number contains 45** then route through SIP Entity at 10.23.142.22
SIP Routing Engine

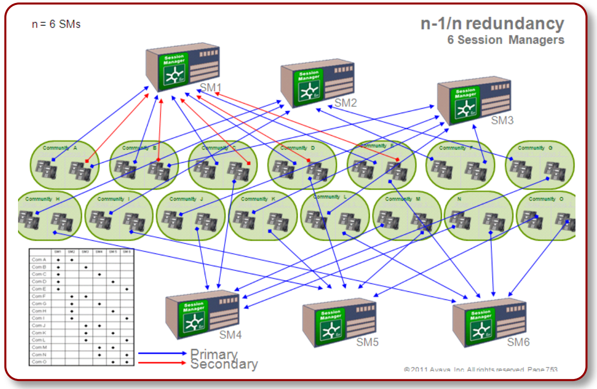
Centralized Sip Routing



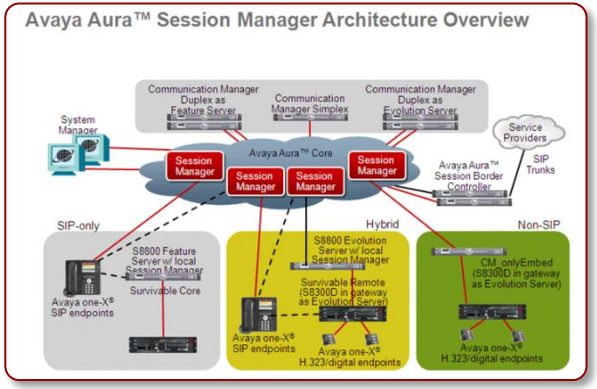
Integration & Adaptation

AVAYA
INTELLIGENT COMMUNICATIONS
Software
SM 100
Certificates, Firewall, Rate Limiting, etc
SM100

SIP Firewall



Scalable


Avaya Aura™ Session Manager Architecture Overview
Communication Manager Duplex as Feature Server
Communication Manager Simplex
Communication Manager Duplex as Evolution Server
System Manager
Service Providers
Avaya Aura™ Core
Session Manager
Session Manager
Session Manager
Session Manager
SIP Trunks
Avaya Aura™ Session Border Controller
SIP-only
Hybrid
Non-SIP
S8800 Feature Server w/ local Session Manager
Survivable Core
Avaya one-X® SIP endpoints
S8800 Evolution Server w/ local Session Manager
Survivable Remote (S8300D in gateway as Evolution Server)
Avaya one-X® SIP endpoints
Avaya one-X® H.323/digital endpoints
CM_onlyEmbed (S8300D in gateway as Evolution Server)
Avaya one-X® H.323/digital endpoints

High Availability & Redundancy

Registration & Authentication

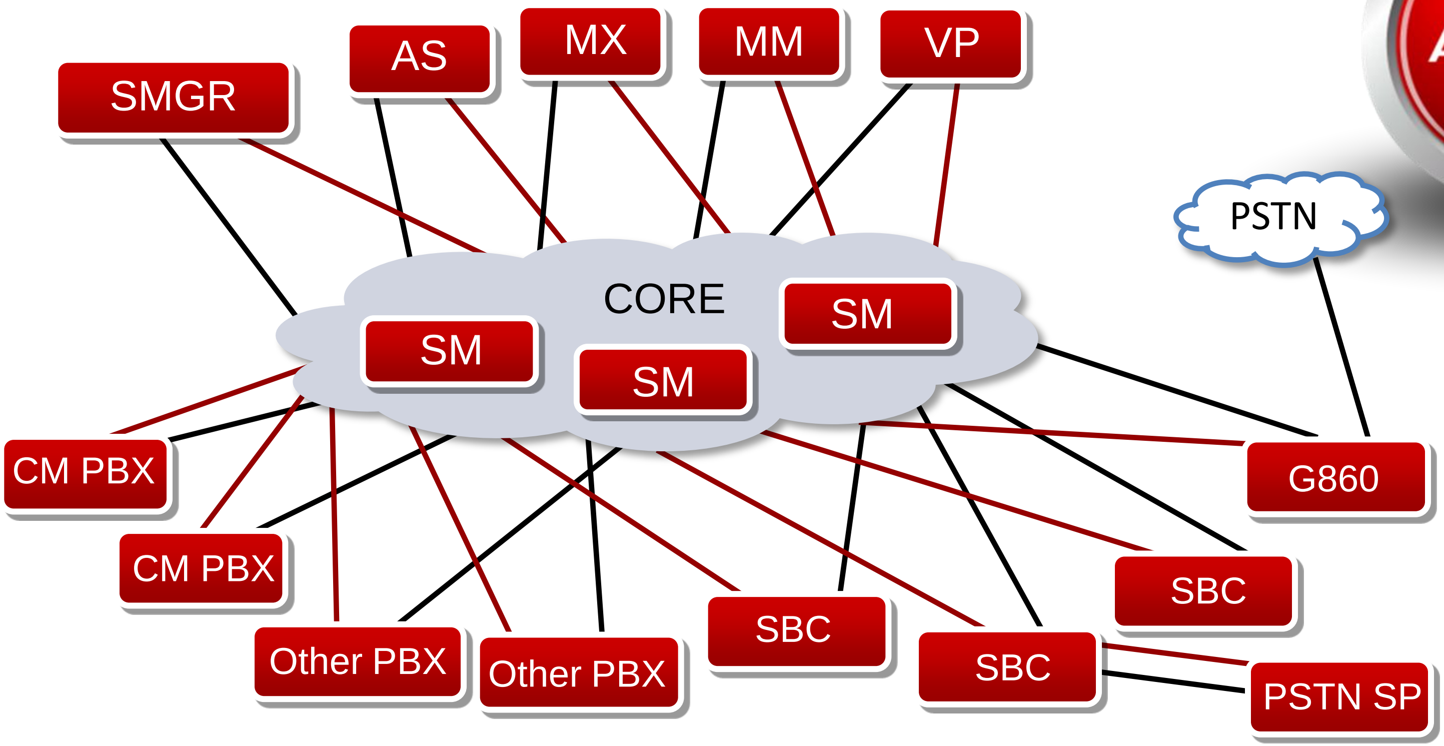
Session Manager Function

Session Manager functions as a sophisticated **Secure SIP Routing Engine**.

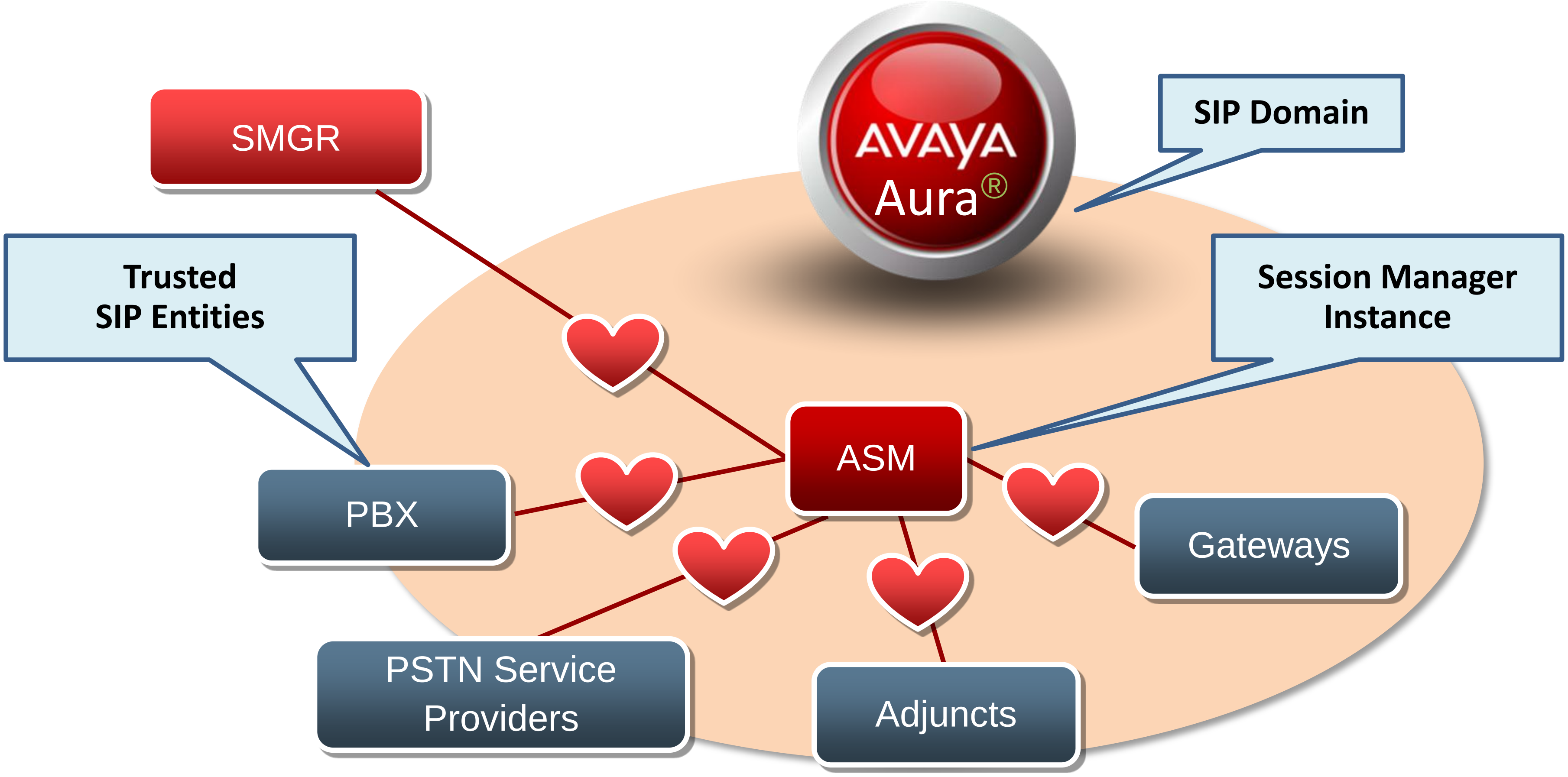
A routing engine that can integrate different telephony systems, and ideal for handling the communications of today's enterprise organizations.

Session Manager as the Avaya Aura® Core

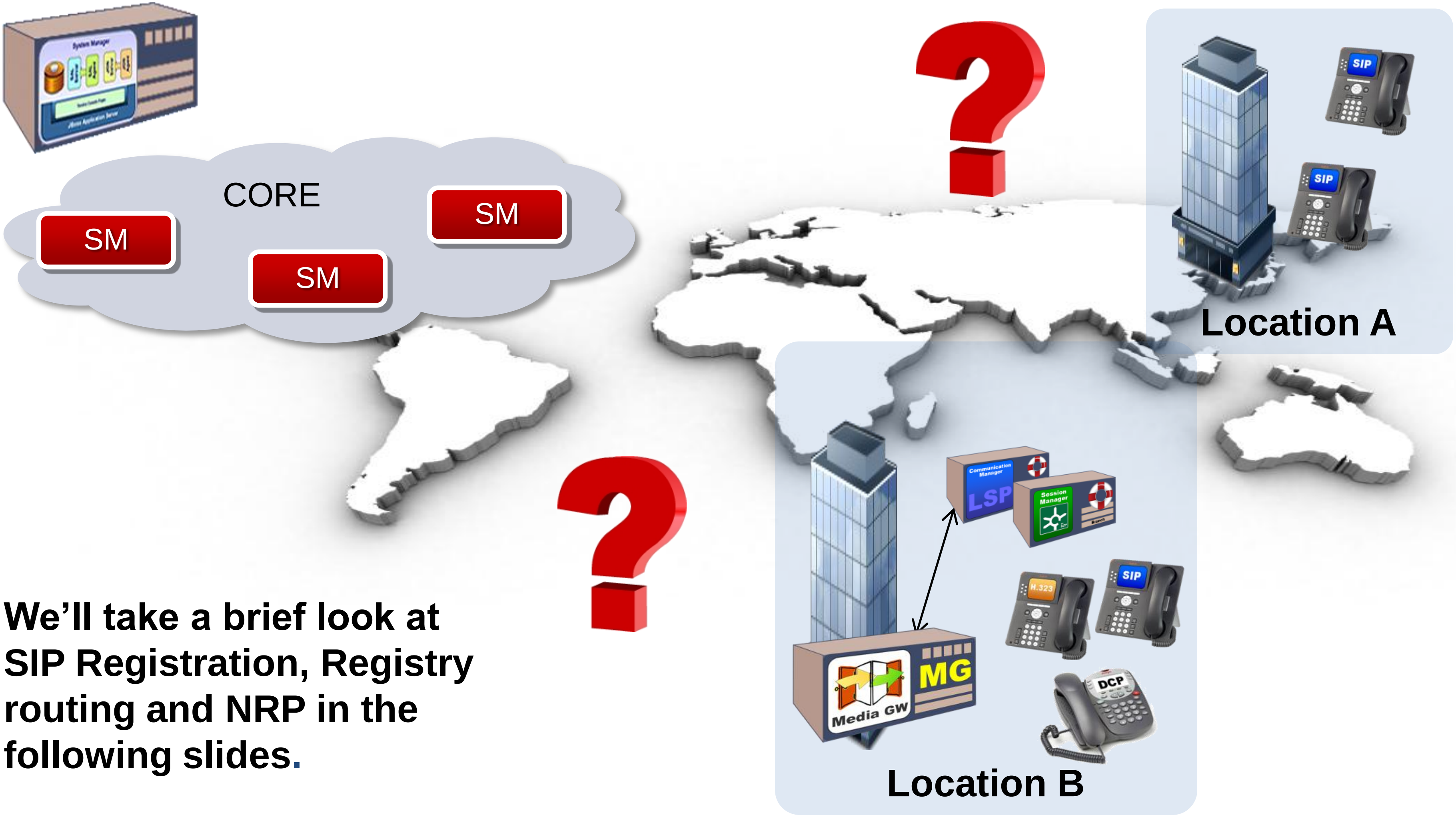
- The core component within the Avaya Aura® solution:
  - Integrates all the SIP entities across the entire enterprise network within a company.
  - Each location, branch, or application is part of the overall enterprise.



Session Manager Instance and SIP Entities

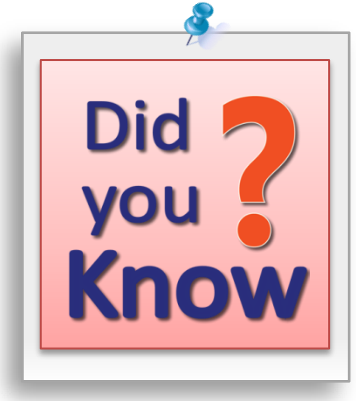


So How Does Session Manager Route Traffic within this IMS Network?



We’ll take a brief look at SIP Registration, Registry routing and NRP in the following slides.

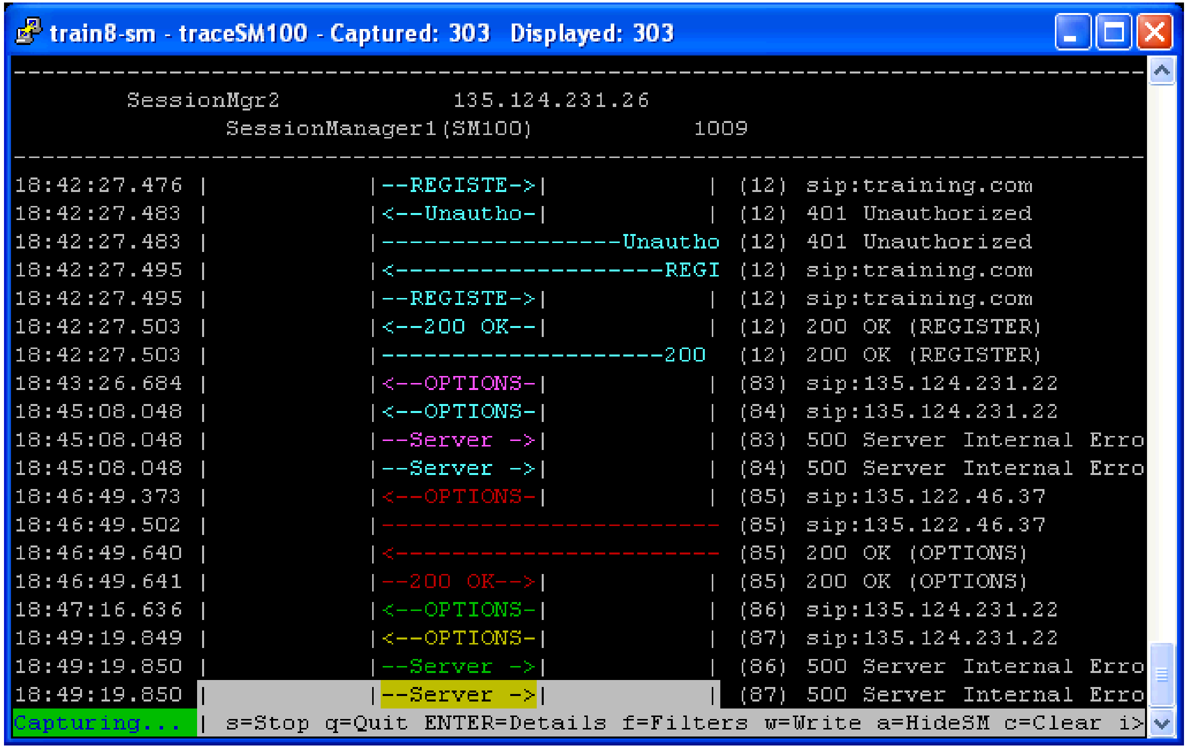
Centralized Routing: SIP Endpoint Registration and Registry Routing



- Ideally all SIP traffic in an enterprise is routed to Session Manager
- Session Manager is responsible for authenticating all SIP endpoints before it will route its SIP session.
- All SIP endpoints require a **SIP Communication Profile** which has its SIP URI (1234@avaya.com) and password
- Once the SIP Endpoint is authenticated Session Manager will store its location info (ip address, SIP URI) for future use.
- If the called party is a SIP endpoint it will authenticate that user and setup the call.
- The two SIP endpoints will negotiate the preferred media type (audio vs video) and protocol (G729? H.264?) used between each other then RTP packets are exchanged.

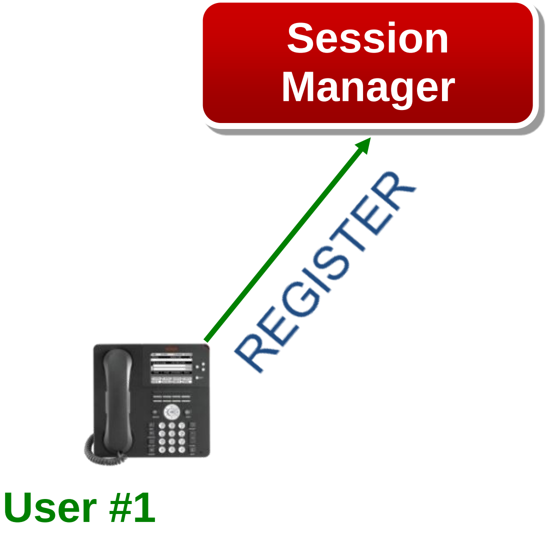
Sample SIP Trace: Registration

- Trace executed using the traceSM tool.
- In this trace, User Agent sent a **REGISTER** request to Session Manager represented by the **SM100 Security Module**



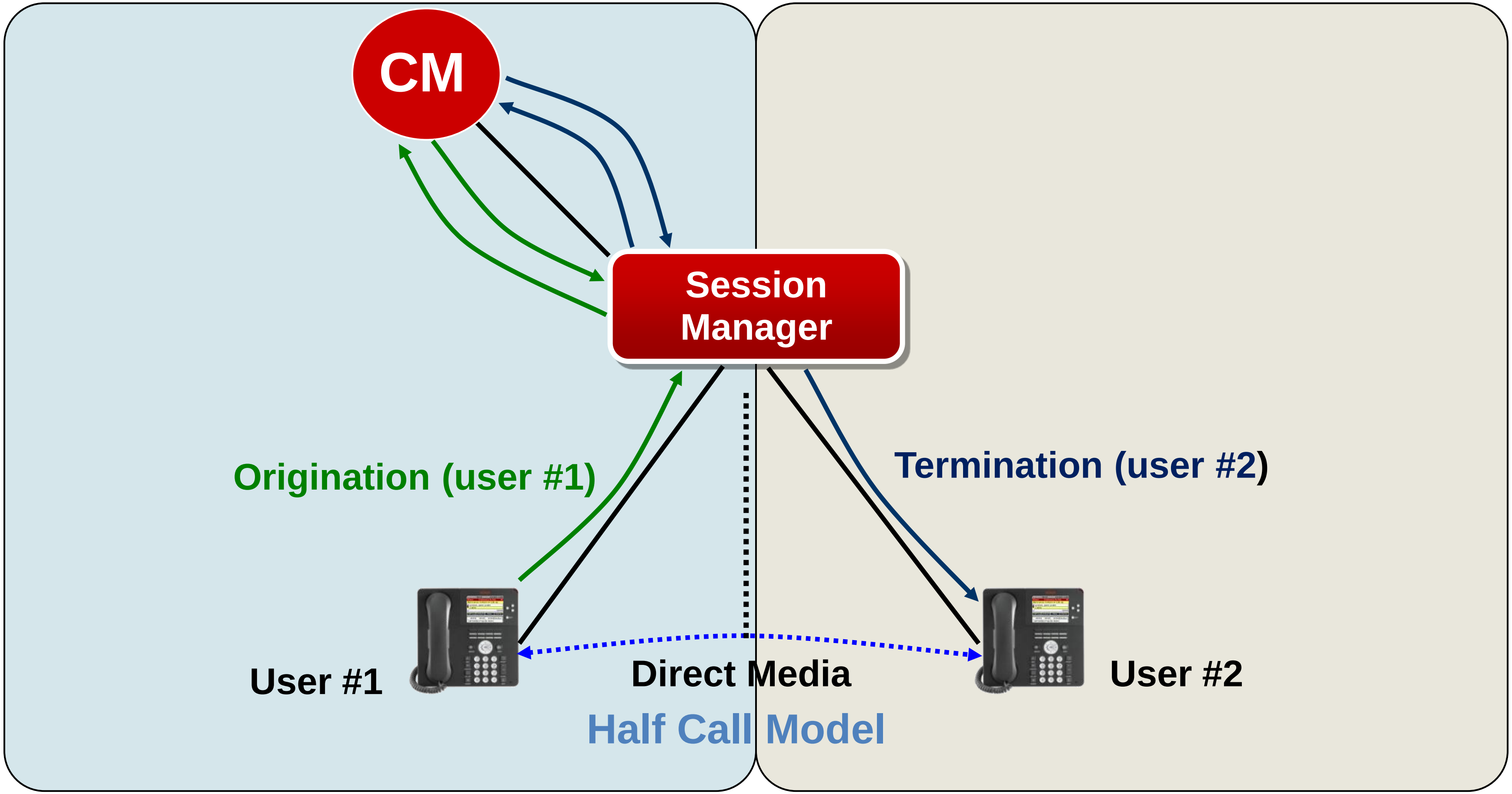
train8-sm - traceSM100 - Captured: 303 Displayed: 303

```
--------------------------------------------------------------------------------
        SessionMgr2             135.124.231.26
               SessionManager1(SM100)           1009
--------------------------------------------------------------------------------
18:42:27.476 |           |--REGISTE->|           |  (12) sip:training.com
18:42:27.483 |           |<--Unautho-|           |  (12) 401 Unauthorized
18:42:27.483 |           |-----------------Unautho (12) 401 Unauthorized
18:42:27.495 |           |<--------------------REGI (12) sip:training.com
18:42:27.495 |           |--REGISTE->|           |  (12) sip:training.com
18:42:27.503 |           |<--200 OK--|           |  (12) 200 OK (REGISTER)
18:42:27.503 |           |--------------------200   (12) 200 OK (REGISTER)
18:43:26.684 |           |<--OPTIONS-|           |  (83) sip:135.124.231.22
18:45:08.048 |           |<--OPTIONS-|           |  (84) sip:135.124.231.22
18:45:08.048 |           |--Server  ->|          |  (83) 500 Server Internal Erro
18:45:08.048 |           |--Server  ->|          |  (84) 500 Server Internal Erro
18:46:49.373 |           |<--OPTIONS-|           |  (85) sip:135.122.46.37
18:46:49.502 |           |------------------------  (85) sip:135.122.46.37
18:46:49.640 |           |<-----------------------  (85) 200 OK (OPTIONS)
18:46:49.641 |           |--200 OK-->|           |  (85) 200 OK (OPTIONS)
18:47:16.636 |           |<--OPTIONS-|           |  (86) sip:135.124.231.22
18:49:19.849 |           |<--OPTIONS-|           |  (87) sip:135.124.231.22
18:49:19.850 |           |--Server  ->|          |  (86) 500 Server Internal Erro
18:49:19.850 |           |--Server  ->|          |  (87) 500 Server Internal Erro
Capturing... | s=Stop q=Quit ENTER=Details f=Filters w=Write a=HideSM c=Clear i>
```



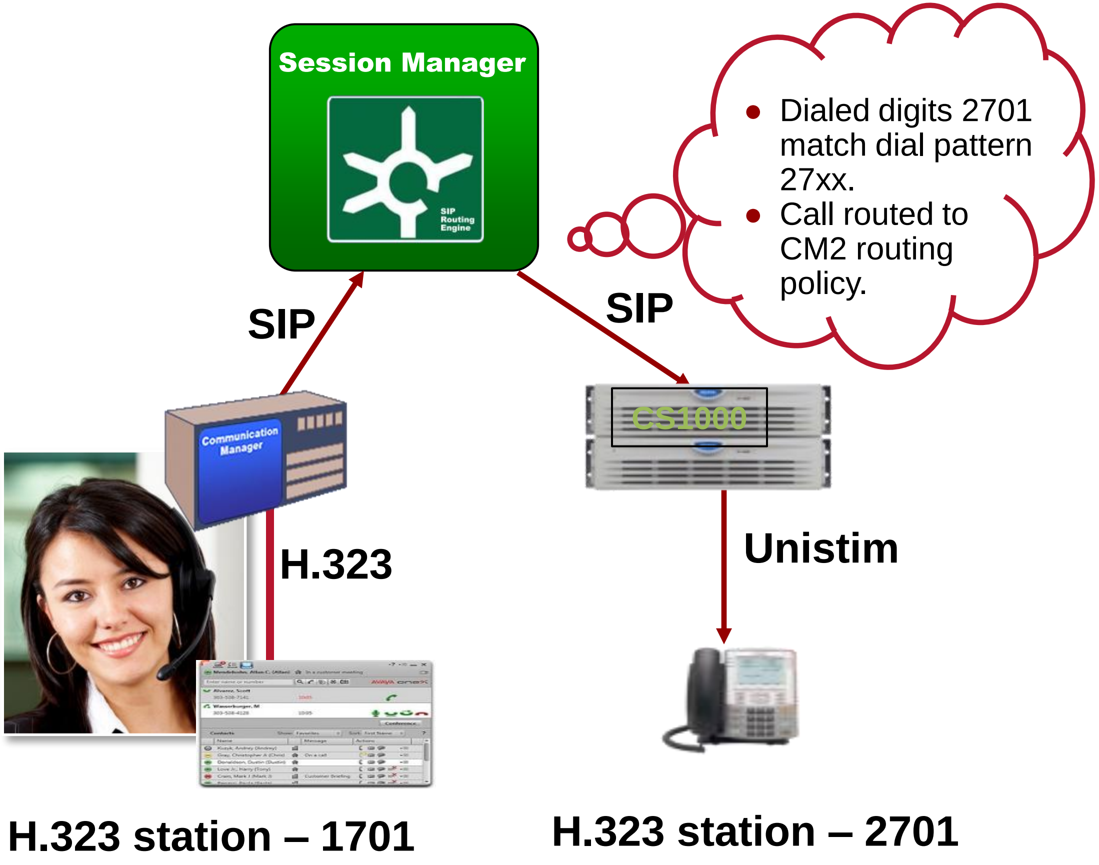
SIP Registry Routing

SIP Registry Routing: SIP to SIP Call Flow



Centralized Routing: Network Routing Policies

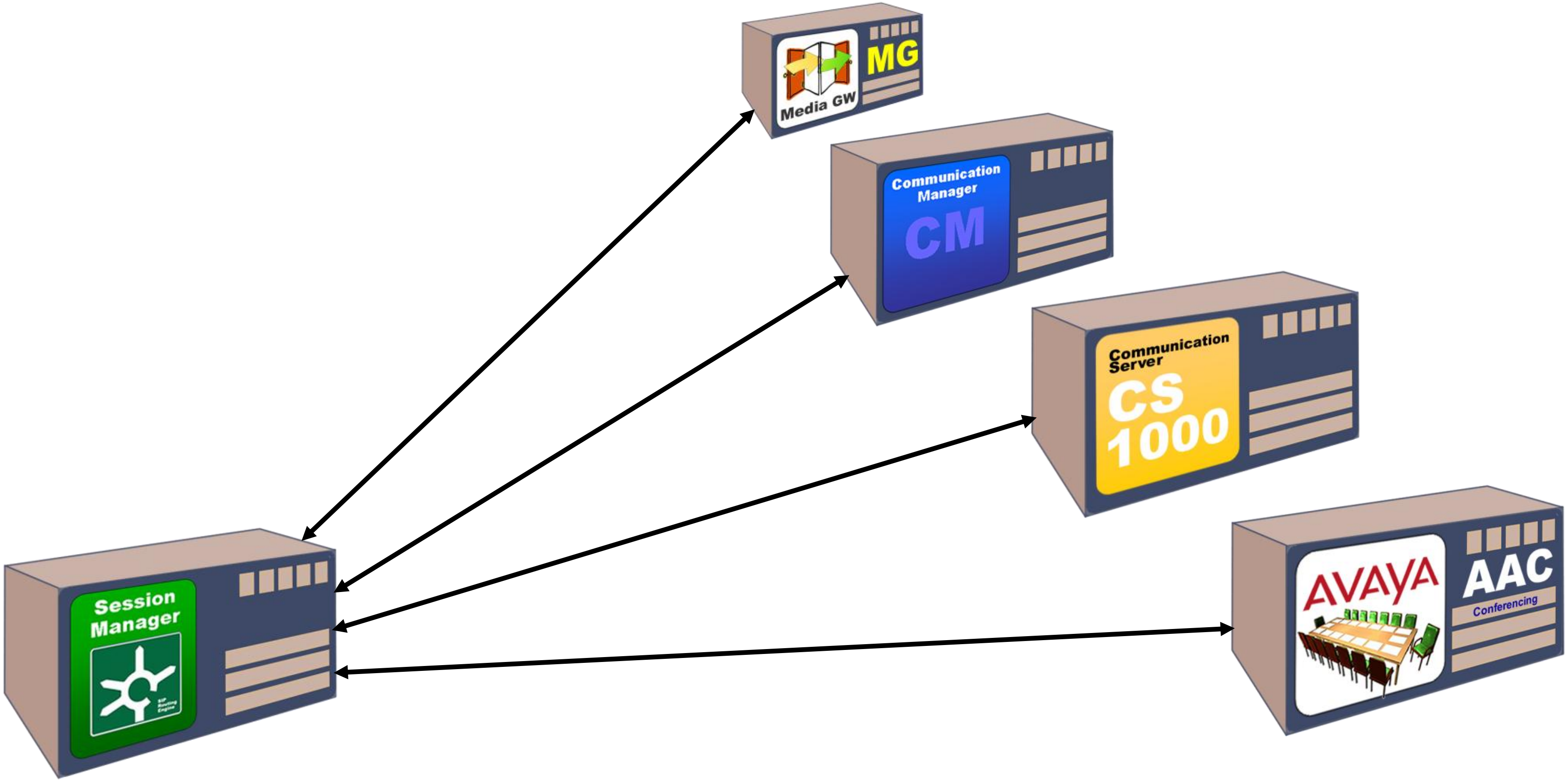
- Session Manager handles routing for non-SIP endpoints differently than it does for SIP endpoints.
- Session Manager uses **dial pattern matching** and **routing policies** for non-SIP endpoints or for routing to SIP endpoints being managed by another Session Manager not within its cluster.



- Dialed digits 2701 match dial pattern 27xx.
- Call routed to CM2 routing policy.

Why doesn't Session Manager use Registry Routing in this scenario?

Session Manager Feature Application Integration

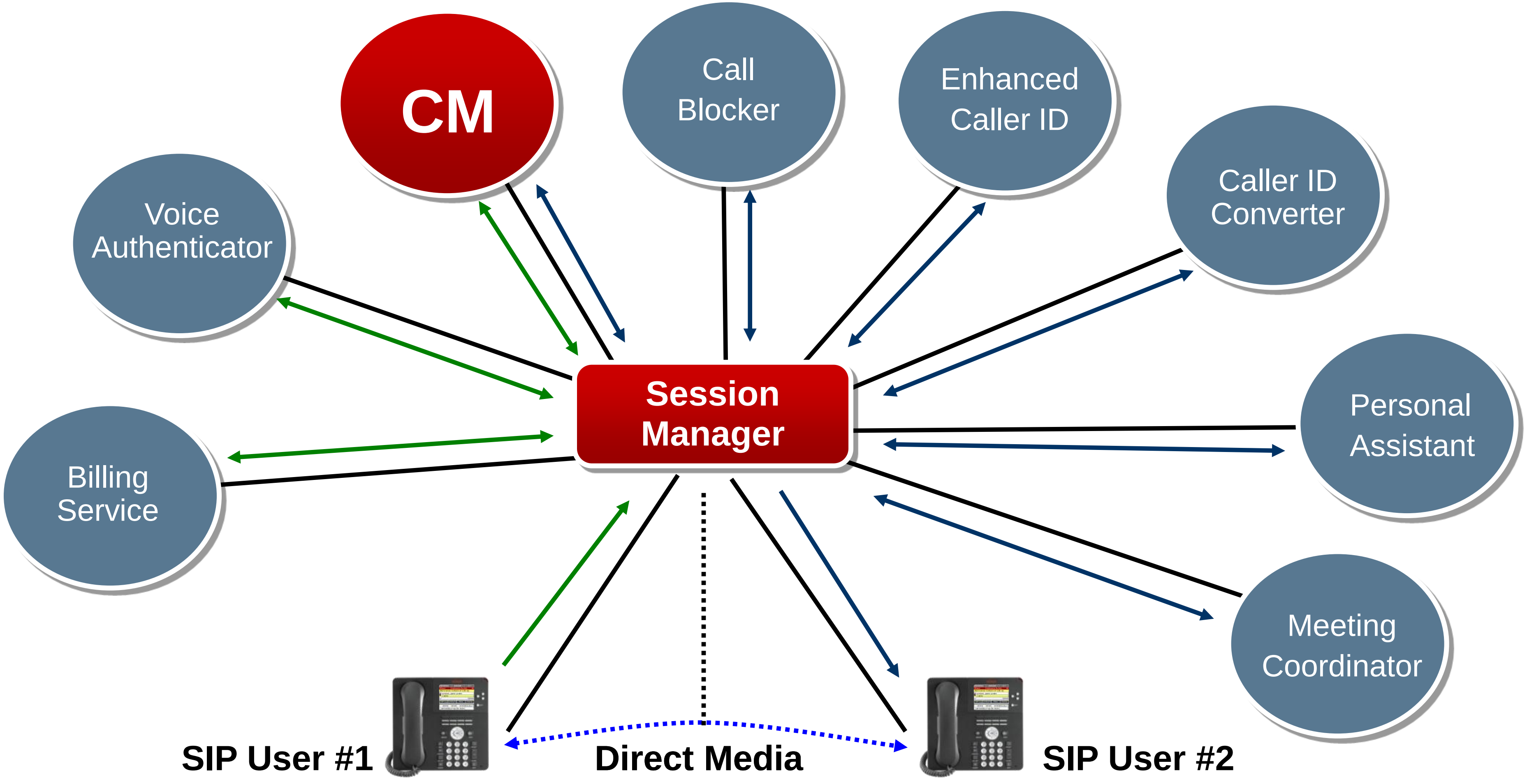


Integration and Adaptation

How does Session Manager process SIP messages from 3rd party vendors that use a different SIP message format?

SIP
Address
Somewhere
Some place
Session
Manager
SIP
Address
Somewhere
Some place
cisco

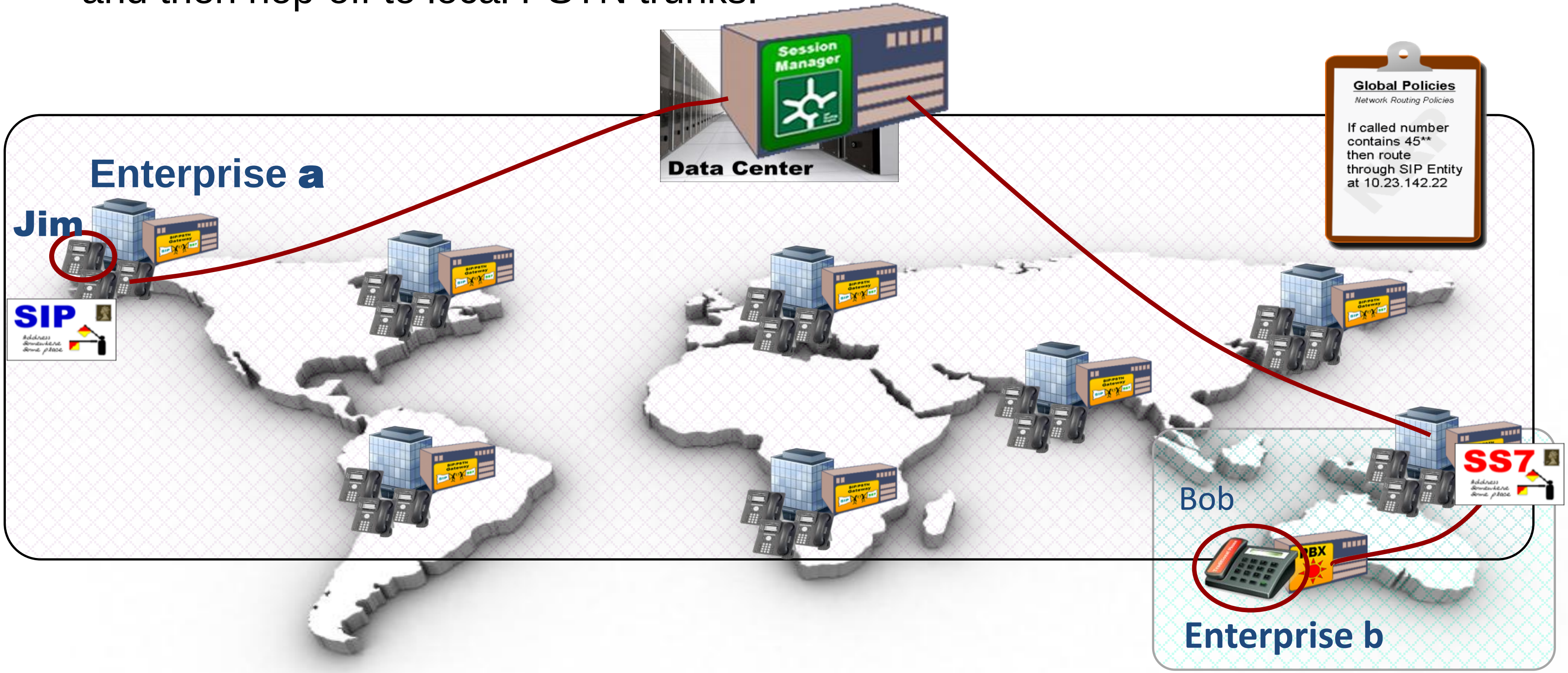
Avaya Aura^{TM} Sequenced Applications in an IMS Network



Half Call Model

Tail-End Hop Off

- Session Manager can be configured to route off-network calls through the WAN and then hop-off to local PSTN trunks.



Global Policies

Network Routing Policies

If called number contains 45** then route through SIP Entity at 10.23.142.22

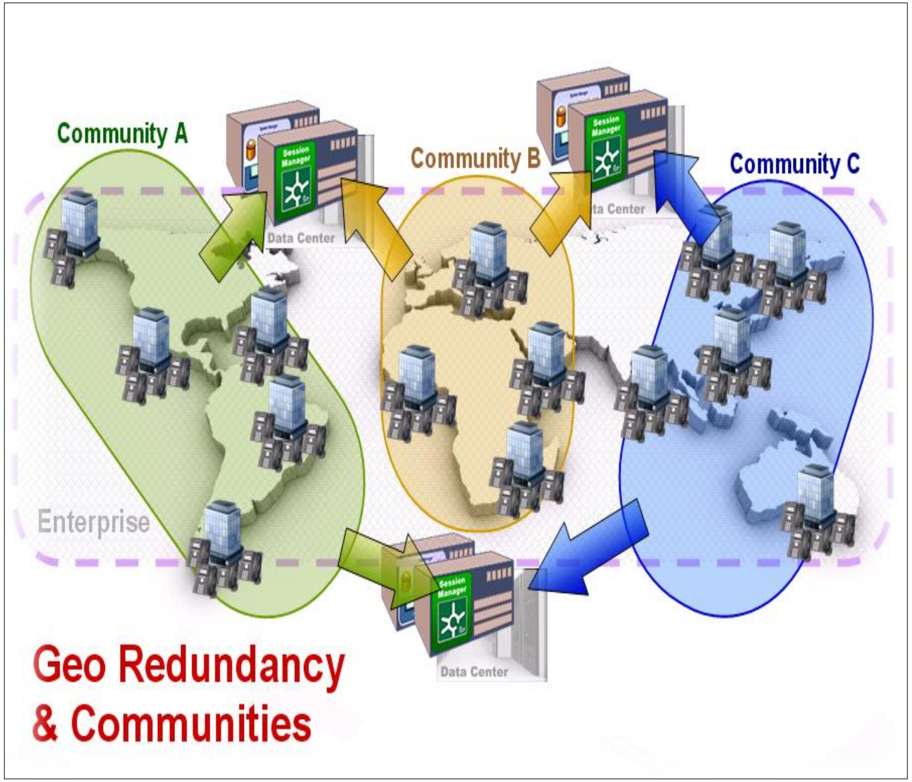
If a dialed number has the international dial code for Australia, and the city code of Sydney, then route to our gateway in Sydney office on IP address 10.24.36.24

PSTN

Short hop – cheaper than long hop

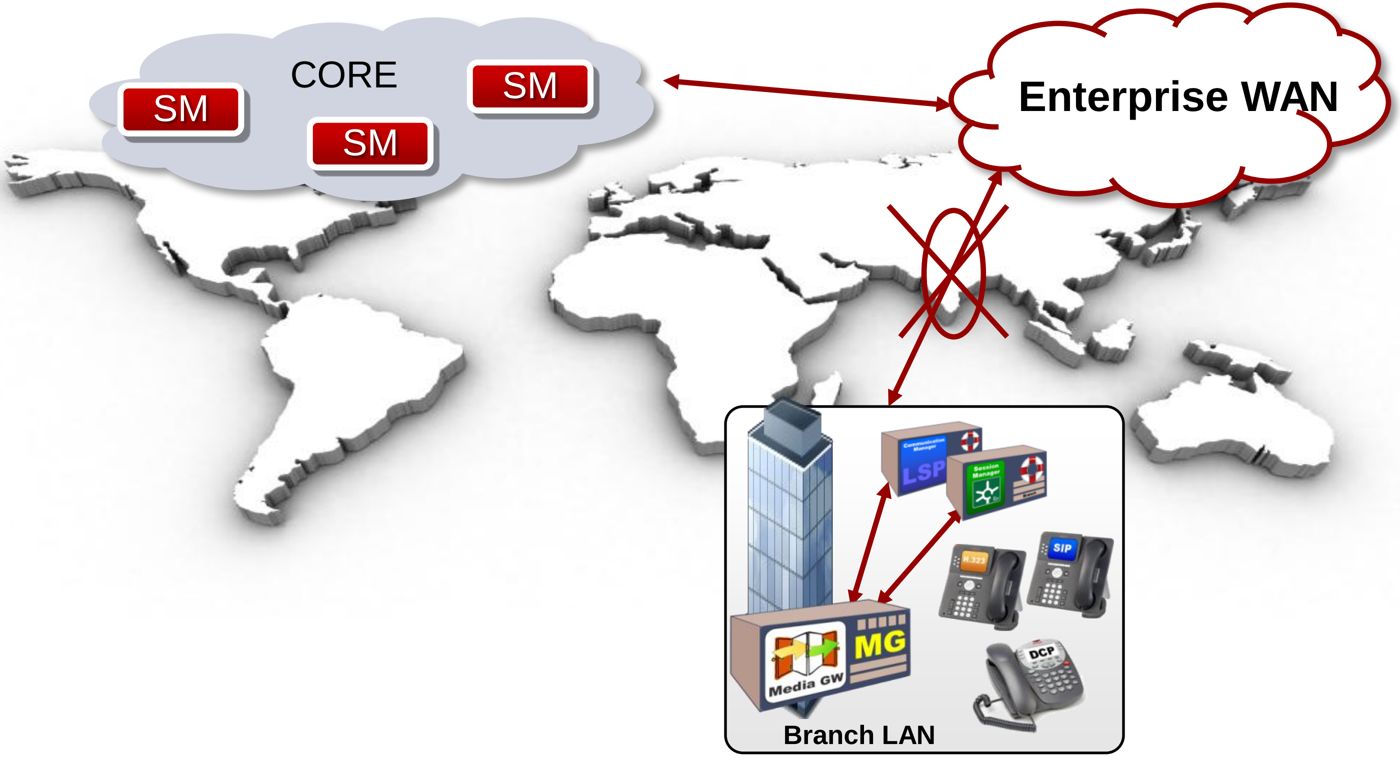
Scale and Redundancy

- Session Manager scales up to 10 instances in the Avaya Aura® Enterprise
- Session Manager can be deployed in an **active-active** configuration to provide load-balancing of user groups/communities where all instances of ASM are actively taking calls.
- When configuring SIP user communication profiles, administrators can assign half of the SIP users in one community to register to ASM1 as its primary and the other half can register to ASM2 as its primary.
- The first half will then be configured to register to ASM2 as its secondary and the second half will register to ASM1 as its secondary.

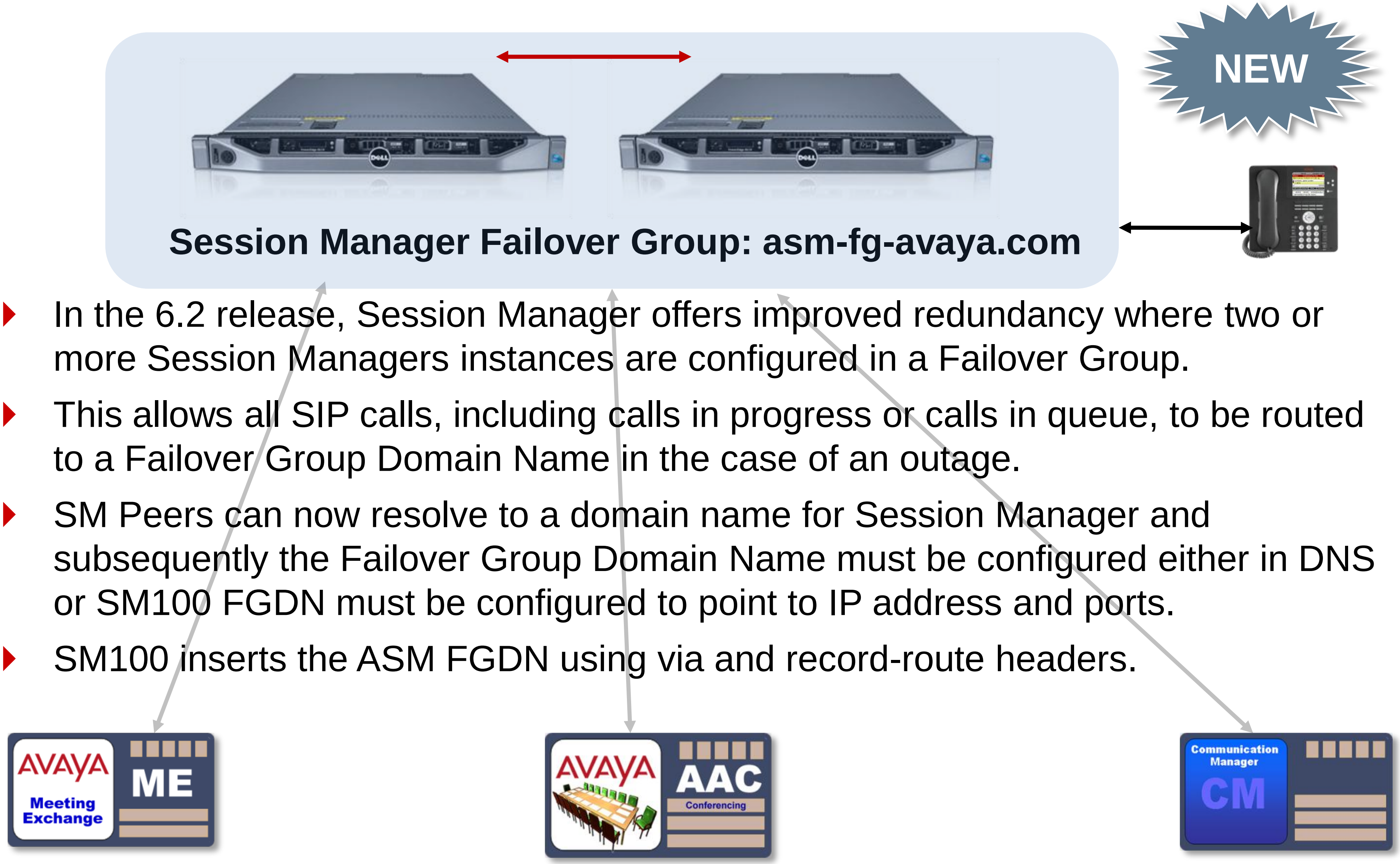


Remote Survivability

- A Remote Survivable instance of Session Manager can be configured as a branch solution.
- Currently being offered as a part of the Embedded CM Survivable Remote Template along with Remote Survivable CM.
- Performs local site SIP message routing, including SIP Registry routing
- Provides connectivity to a local feature processor within the local site



Failover



Session Manager Failover Group: asm-fg-avaya.com

- In the 6.2 release, Session Manager offers improved redundancy where two or more Session Managers instances are configured in a Failover Group.
- This allows all SIP calls, including calls in progress or calls in queue, to be routed to a Failover Group Domain Name in the case of an outage.
- SM Peers can now resolve to a domain name for Session Manager and subsequently the Failover Group Domain Name must be configured either in DNS or SM100 FGDN must be configured to point to IP address and ports.
- SM100 inserts the ASM FGDN using via and record-route headers.

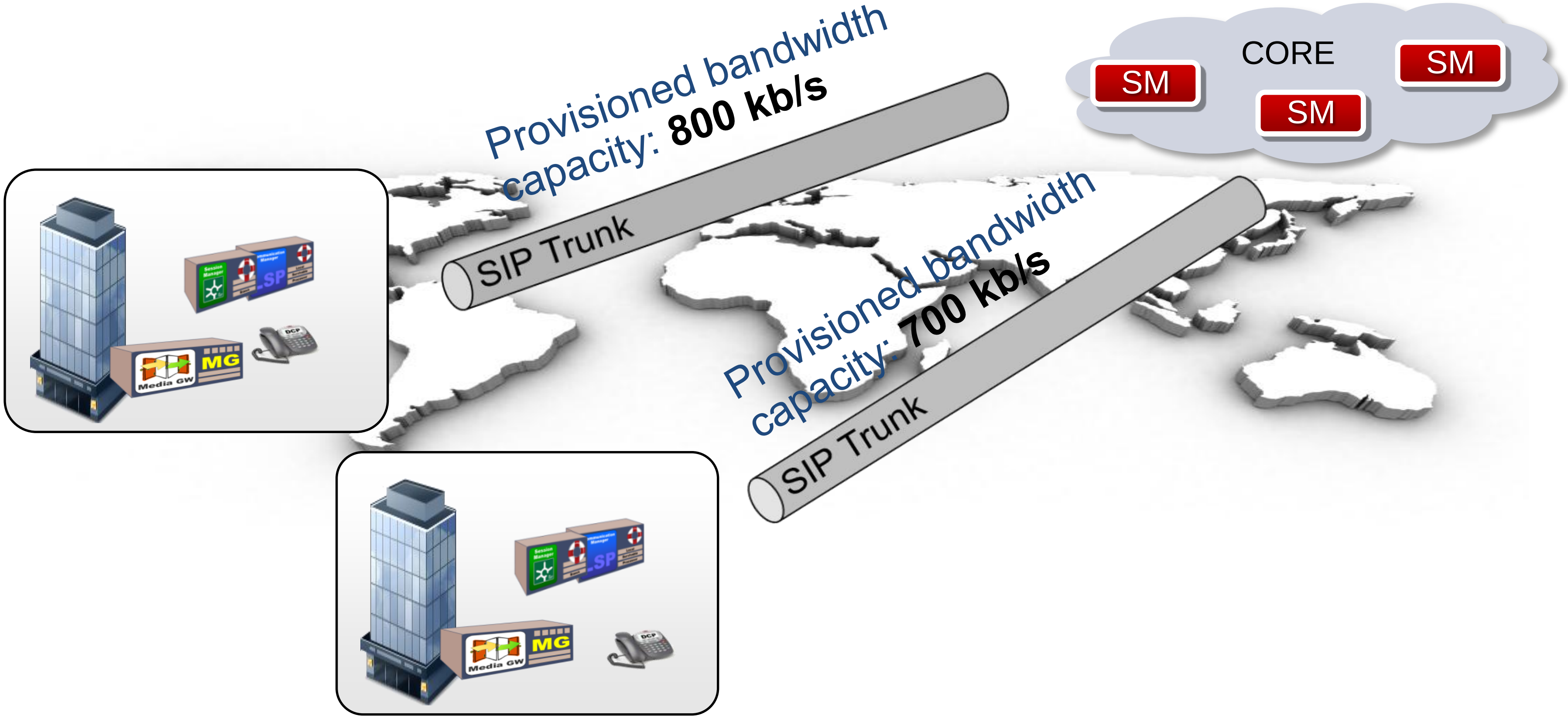
Capacity and Performance

Avaya Aura® Quick Reference Specifications			
Item	**R6.0**	**R6.1**	**R6.2**
Total Enterprise SIP Users	50,000	100,000	100,000
Total Enterprise Users	100,000	100,000	**250,000**
SIP Users/SM	10,000	12,000	12,000
SIP Users/CM	18,000	18,000	**36,000**
Total Enterprise Presence Users	45,000	81,000	81,000
Presence Users/SM	7,000	9,000	9,000
TLS Connections	50,000	100,000	100,000
SM Instances	6	10	10
BHCC per SM	250,000	300,000	**350,000***
Simultaneous Sessions	65,000	80,000	**90,000***
Registrations/Second per SM	NA	NA	**800**
Advanced SIP Terminal Initializations/Second per SM	NA	NA	**10****
Survivable Remotes	250	250	250
Communication Managers	500	500	500
Locations/Adaptations/SIP Entities	25,000	25,000	25,000
SIP Domains	1000	1000	1000
Dial Patterns/Routing Policies	250,000	300,000	300,000

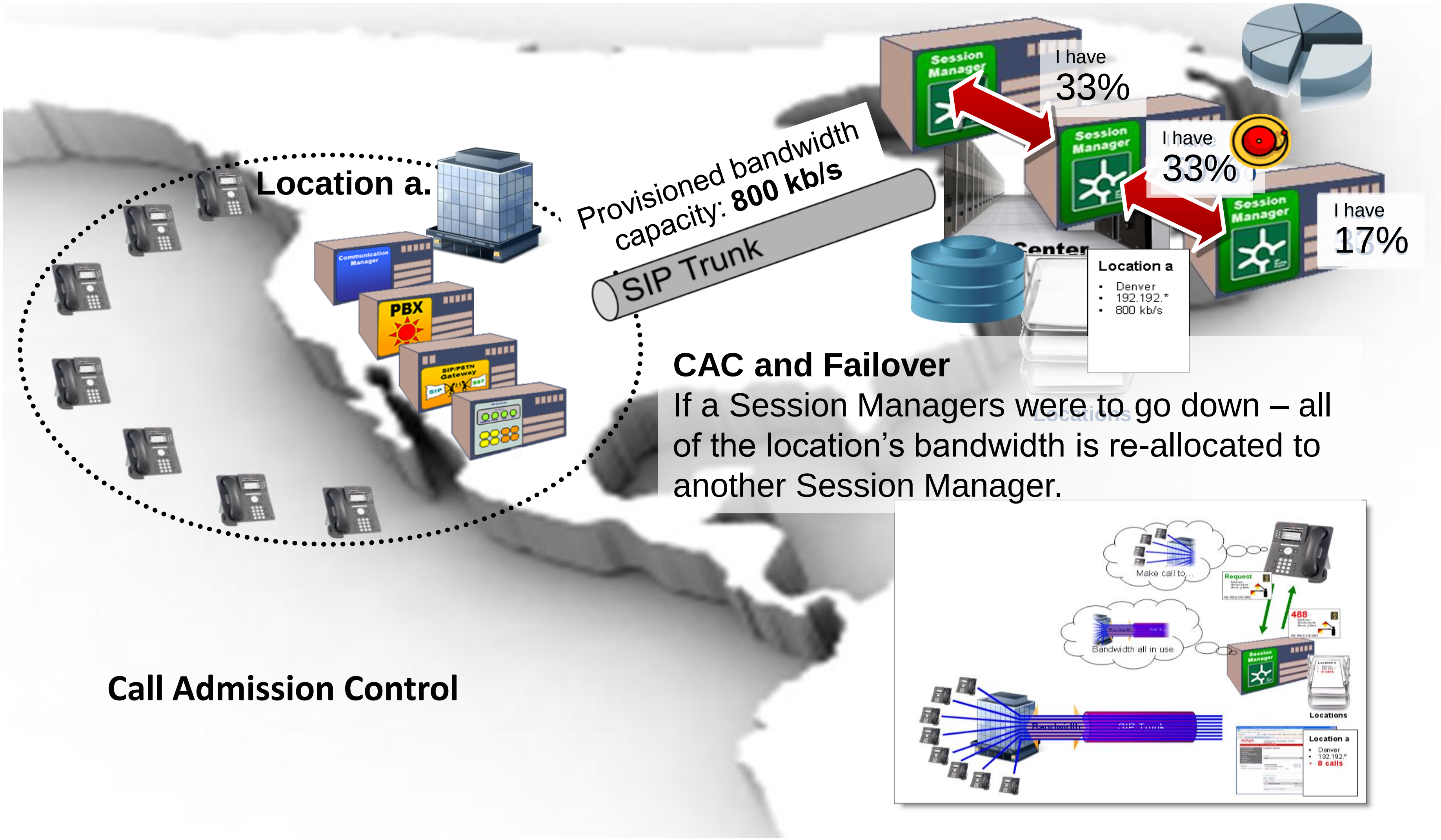
* Preliminary, Subject to Final Confirmation
** Intentionally Throttled for a Single CM

Call Admission Control

- Session Manager has the ability to manage bandwidth to each of its locations using the Call Admissions Control Feature.


CORE
SM
SM
SM
Provisioned bandwidth capacity: 800 kb/s
SIP Trunk
Provisioned bandwidth capacity: 700 kb/s
SIP Trunk
MG
Media GW
SP
DCP
MG
Media GW
SP
DCP

Call Admission Control (continued)

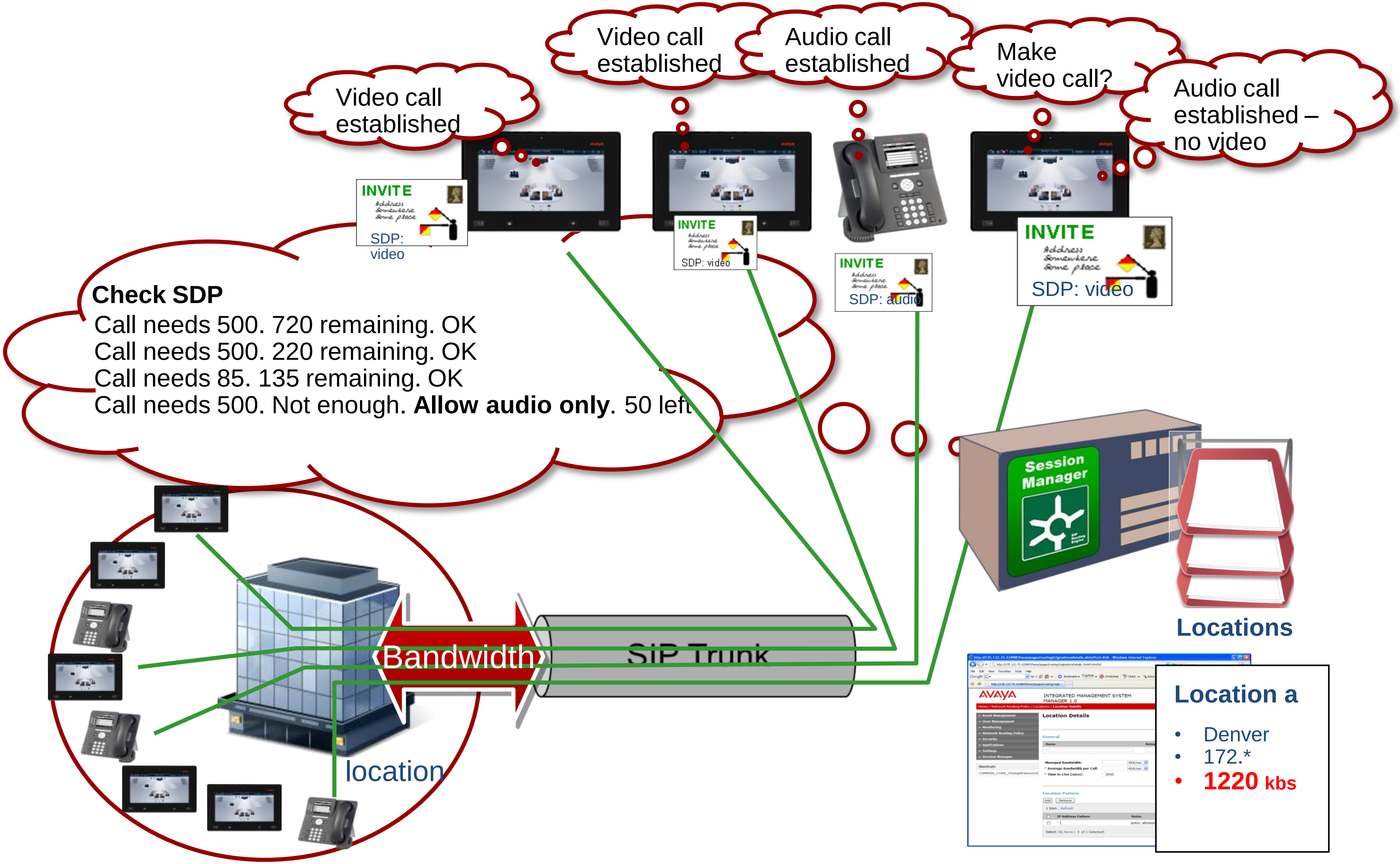


CAC and Failover

If a Session Managers were to go down – all of the location's bandwidth is re-allocated to another Session Manager.

Call Admission Control

SM 6.1 Call Admission Control Down-Sizing



Check SDP

Call needs 500. 720 remaining. OK
Call needs 500. 220 remaining. OK
Call needs 85. 135 remaining. OK
Call needs 500. Not enough. **Allow audio only**. 50 left

http://135.122.75.42/NRP/faces/pages/routingOriginationsDetails.xhtml?cid=826 - Windows Internet Explorer

AVAYA INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Home / Network Routing Policy / Locations / Location Details

- Asset Management
- User Management
- Monitoring
- Network Routing Policy
- Security
- Applications
- Settings
- Session Manager

Shortcuts
COMMON_CONS_ChangePassword

Location Details

General

Name | Notes

Managed Bandwidth: Kbit/sec
* Average Bandwidth per Call: Kbit/sec
* Time to Live (secs): 3600

Location Pattern

Add | Remove

1 Item | Refresh

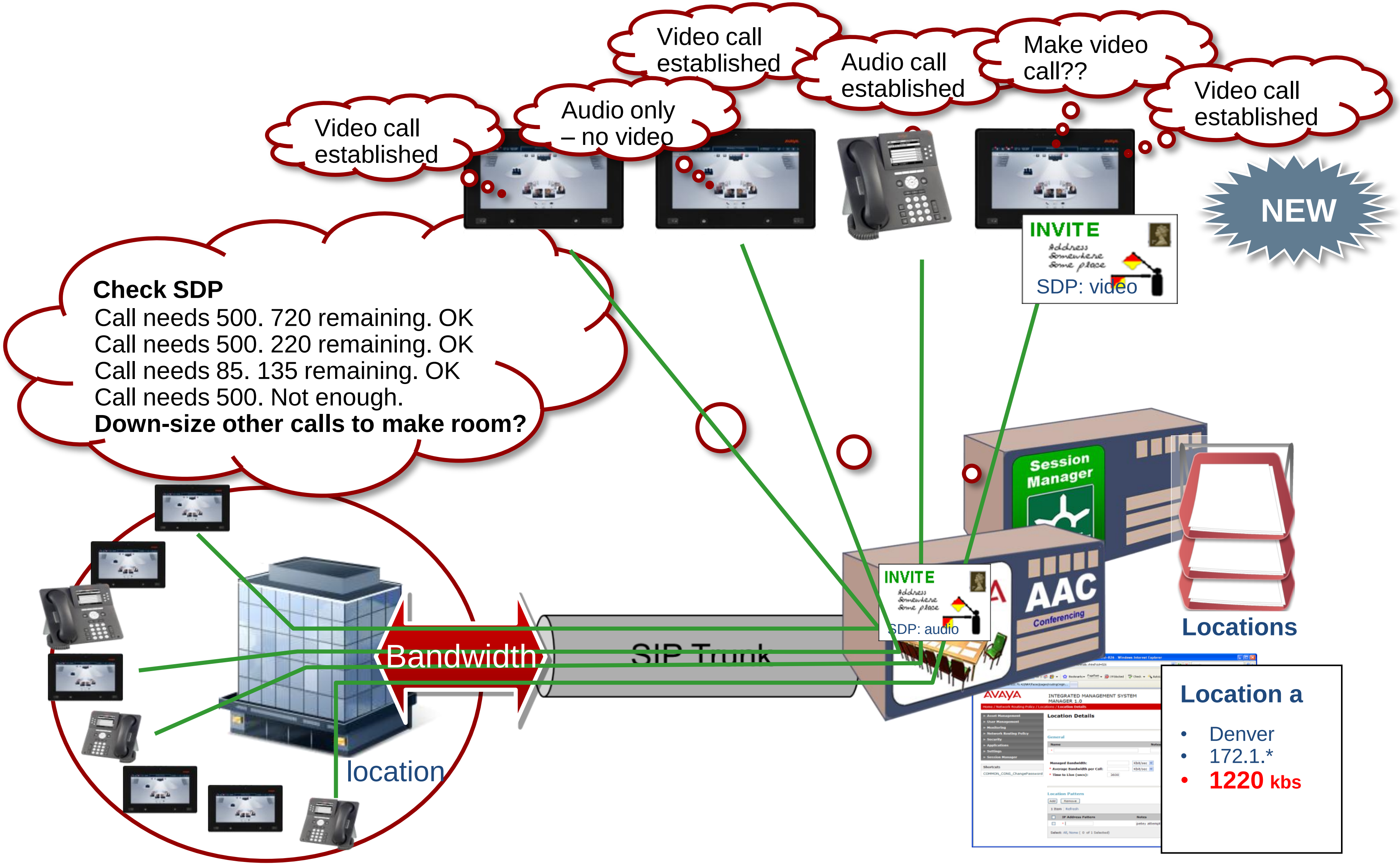
IP Address Pattern	Notes
*	petey attempt

Select: All, None (0 of 1 Selected)

Location a

- Denver
- 172.*
- 1220 kbs

SM 6.2 Call Admission Control Mid-Call Down-Sizing



Check SDP
Call needs 500. 720 remaining. OK
Call needs 500. 220 remaining. OK
Call needs 85. 135 remaining. OK
Call needs 500. Not enough.
Down-size other calls to make room?

Location a

- Denver
- 172.1.*
- **1220 kbs**

Improved User Feed-Back

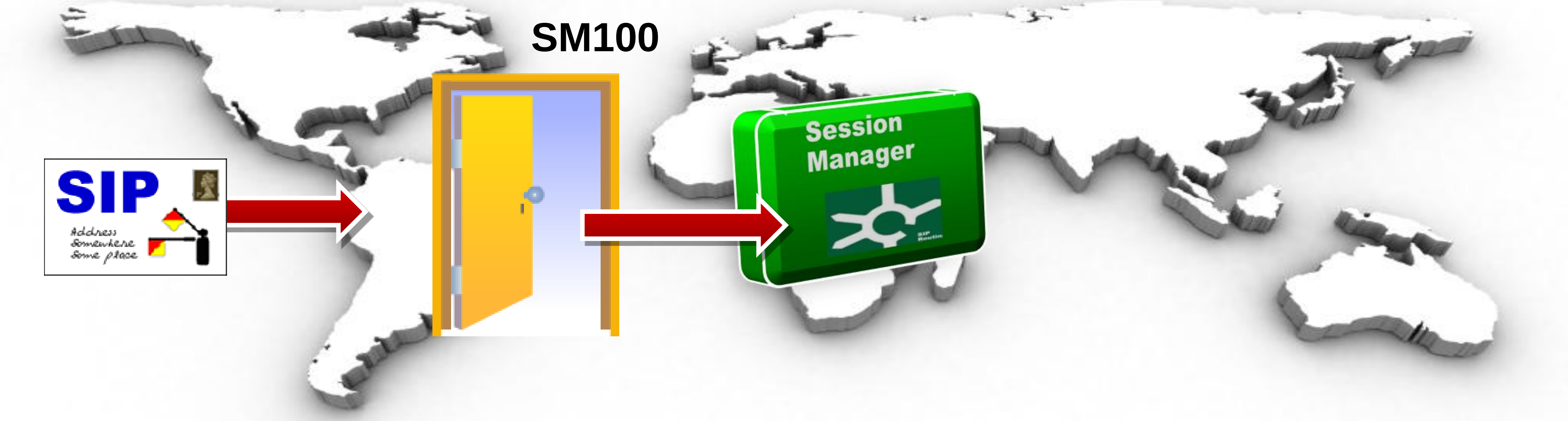
Now I can see when Session Manager downsizes or rejects a call!!

Insufficient bandwidth – please retry later!
Video session speed reduced due to limited bandwidth!

NEW

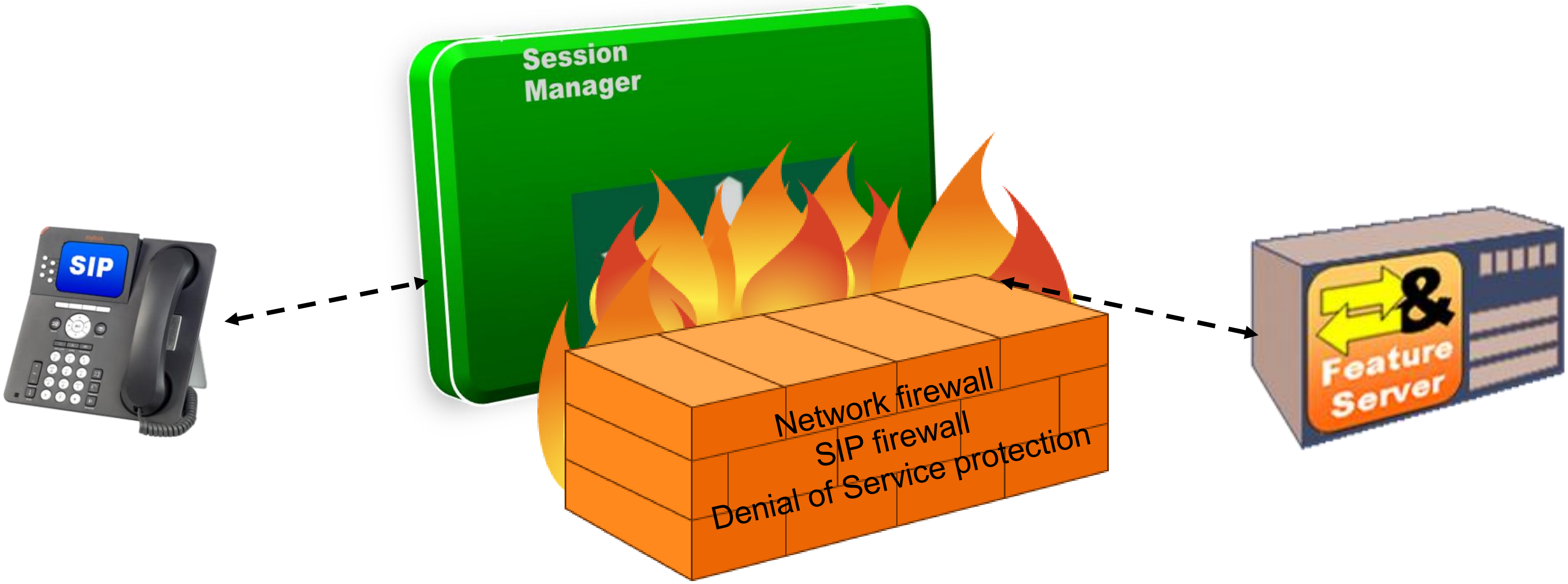
Session Manager Security

- Session Manager handles security primarily through the SM100 Module.
- It is the front door of Session Manager acting as a SIP Firewall, denying or granting access to all SIP traffic.



SM100

- The SM100 off loads most of the heavy security processing and provides a framework for Session Manager security.



SIP/TLS Connections

Questions and Answers

AVAYA | LEARNING

Module 3

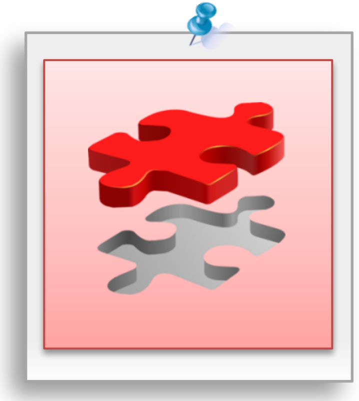
Initial Server Configuration

Module Duration: 45 minutes

Module Objectives

After completing this module, you will be able to:

- Complete Session Manager Initial Server Configuration.



Module Duration:

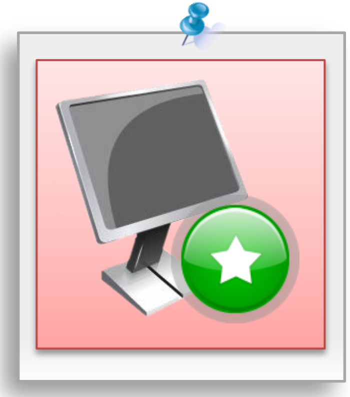
Lesson Objectives

After completing this lesson, you will be able to build the SIP Network components:

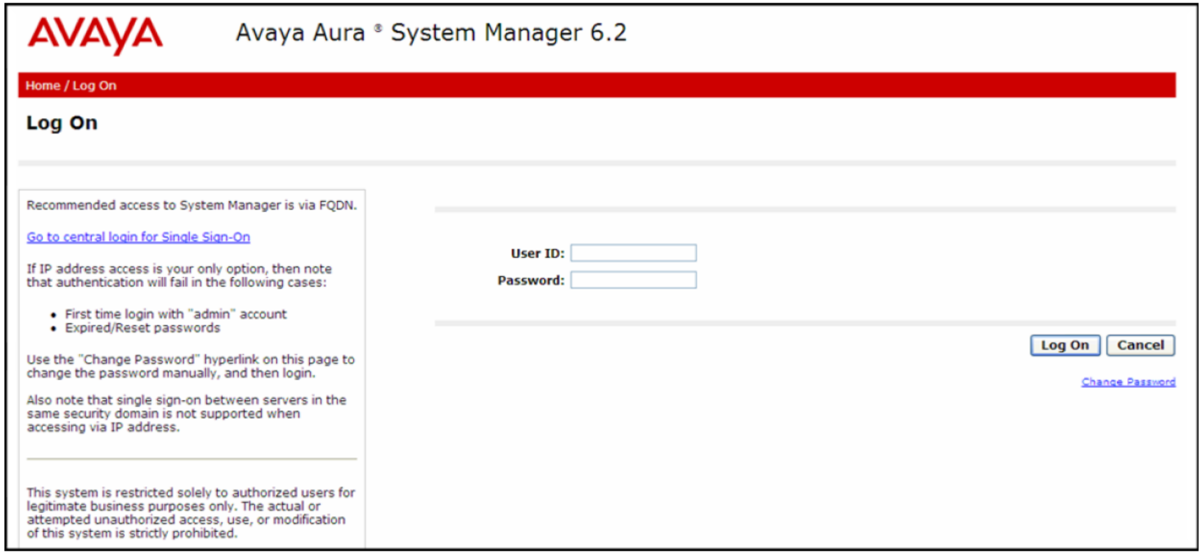
- Define the Secure SIP Domain
- Define a Location
- Define Session Manager SIP Entity
- Define Session Manager Instance
- Enable Session Manager to Accept Services
- Complete Post-Configuration Checks

Lesson Duration:

Exercise: Access System Manager Web Console



Step	Action
1	Log into the System Manager web console by clicking on the Internet Explorer icon on the desktop
2	Point browser to**: https://172.16.x.103**
3	Login: **admin** Password: **Passw0rd!**
4	Select ***Log On***



AVAYA Avaya Aura ® System Manager 6.2

Home / Log On

Log On

Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

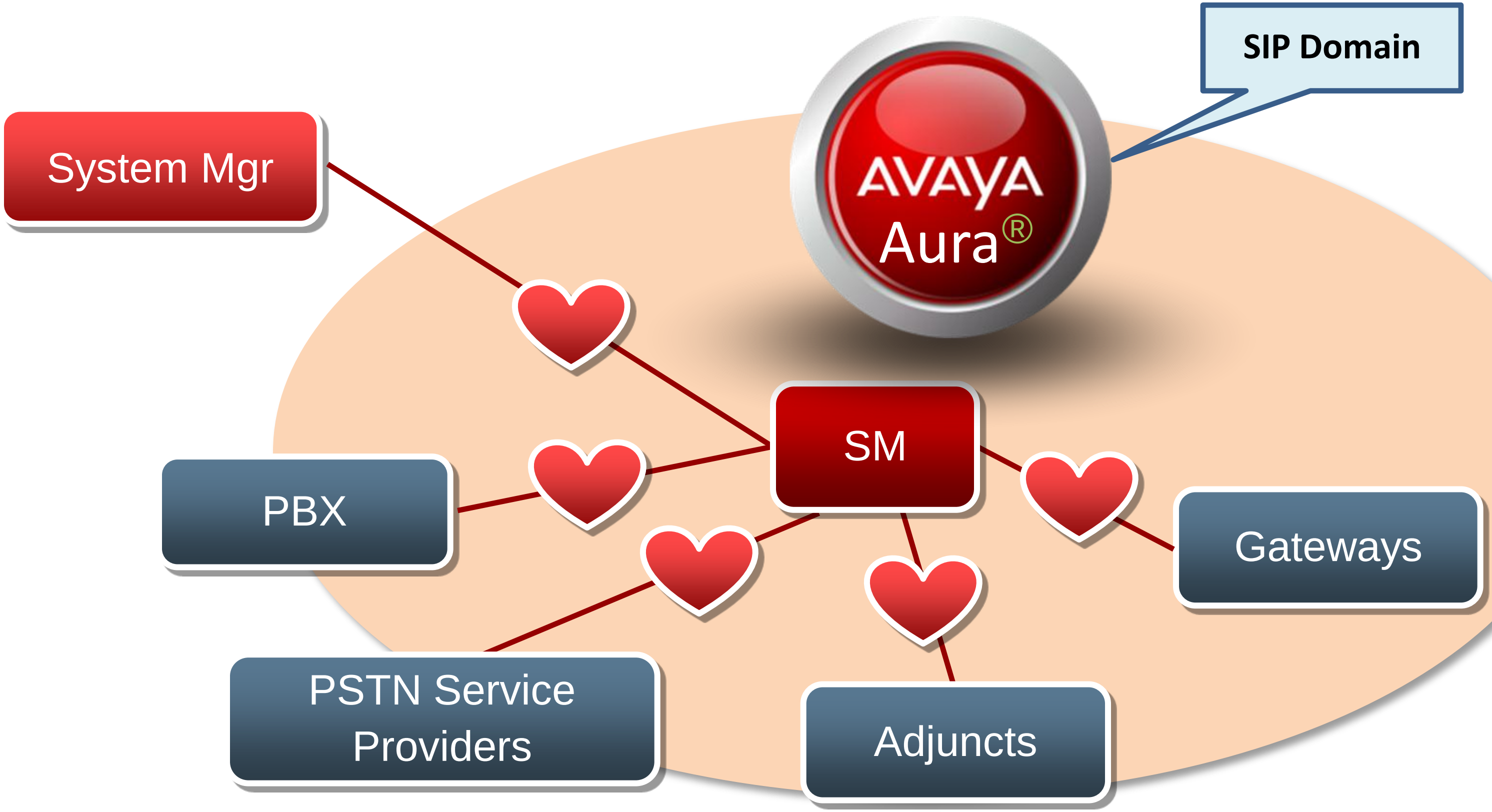
Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

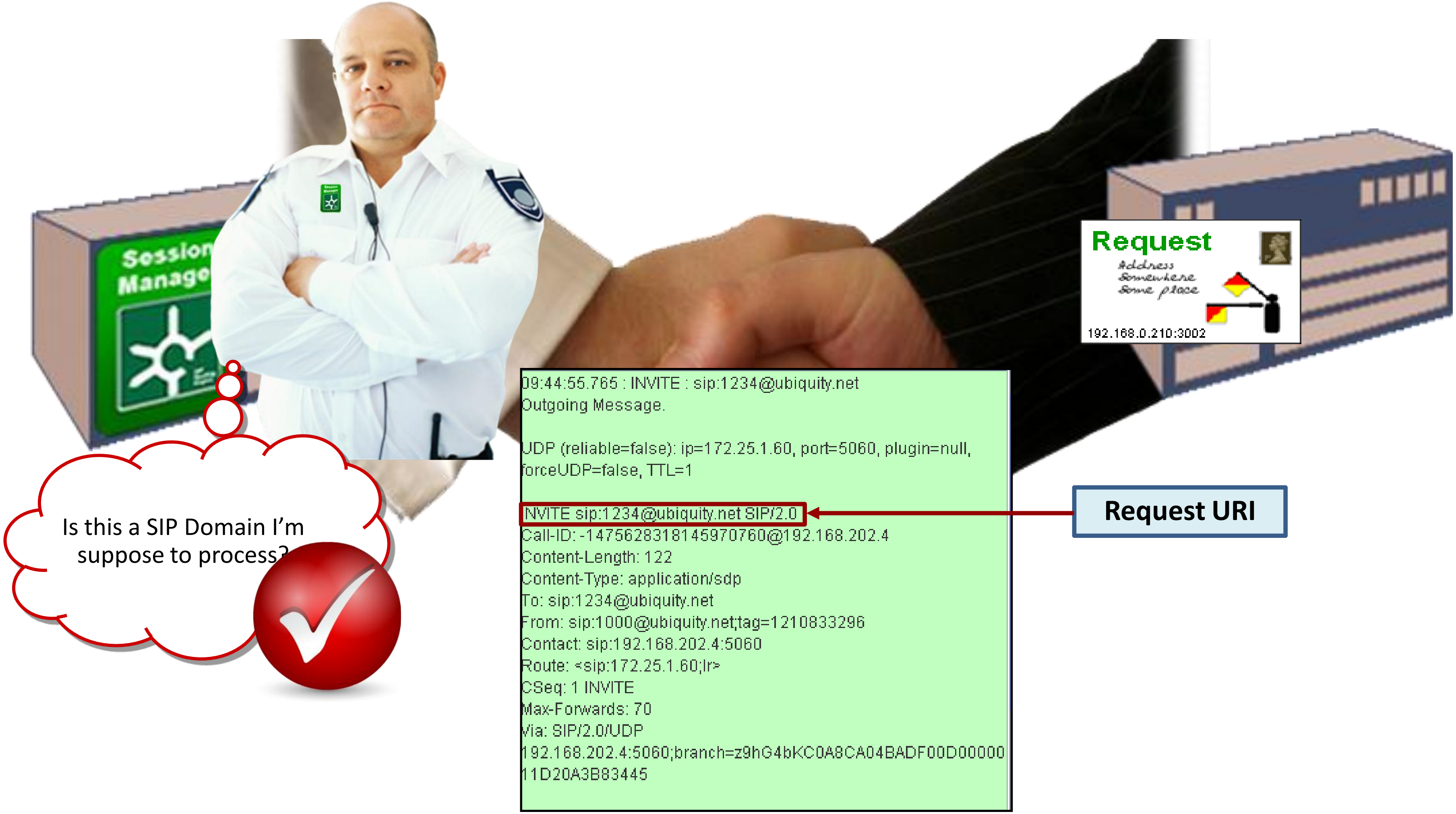
SIP Domains

- In the next exercise we will be creating the secure SIP domain in which Session Manager is at the core, facilitating centralized routing and integration.
- SIP domains are used within Session Manager to enable domain-based routing.
- This increases the enterprise’s flexibility in defining call routing architectures.



SIP Domains (continued)

- Before we can configure routing, we must first create the SIP Domain.

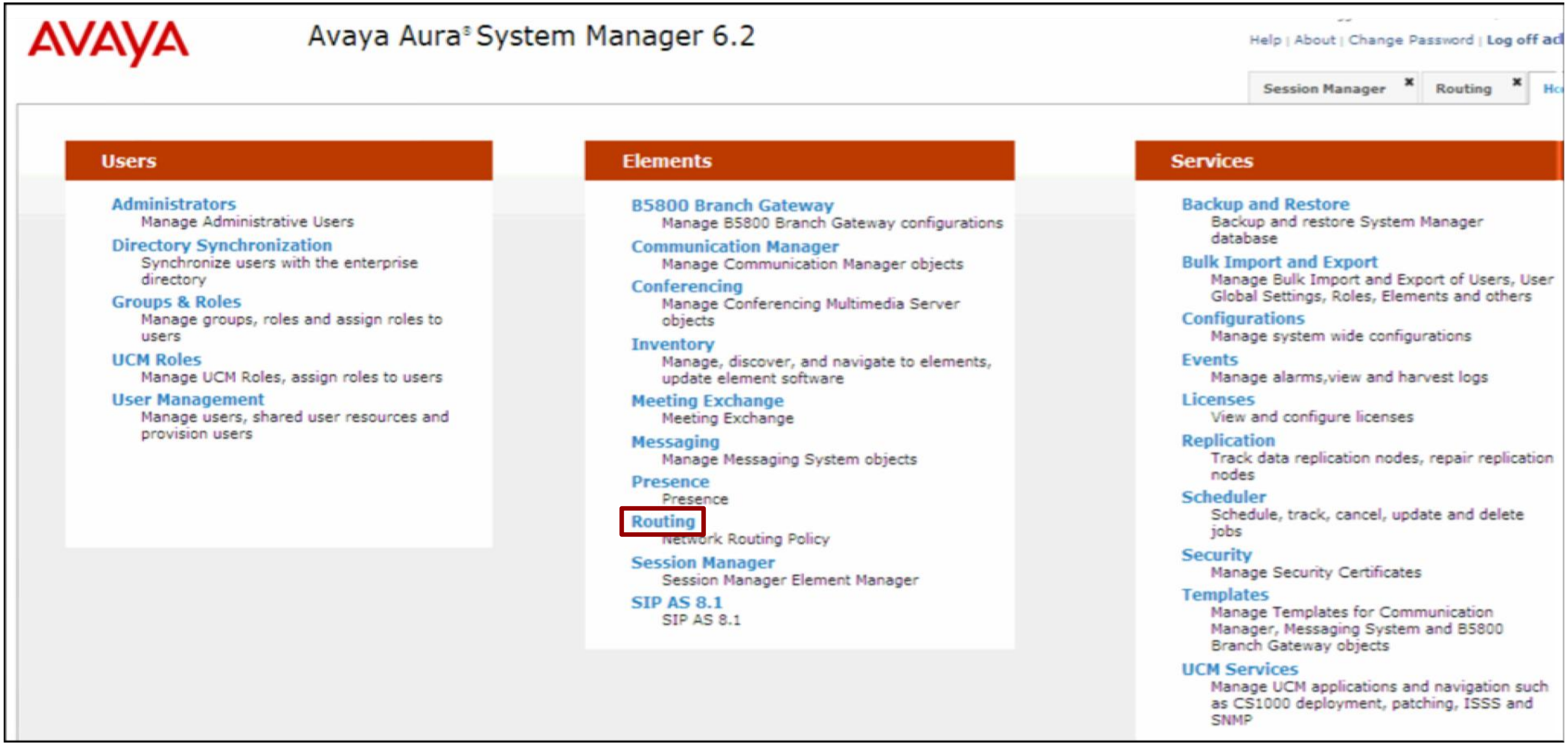


```
09:44:55.765 : INVITE : sip:1234@ubiquity.net
Outgoing Message.

UDP (reliable=false): ip=172.25.1.60, port=5060, plugin=null,
forceUDP=false, TTL=1

NVITE sip:1234@ubiquity.net SIP/2.0
Call-ID: -1475628318145970760@192.168.202.4
Content-Length: 122
Content-Type: application/sdp
To: sip:1234@ubiquity.net
From: sip:1000@ubiquity.net;tag=1210833296
Contact: sip:192.168.202.4:5060
Route: <sip:172.25.1.60;lr>
CSeq: 1 INVITE
Max-Forwards: 70
Via: SIP/2.0/UDP
192.168.202.4:5060;branch=z9hG4bKC0A8CA04BADF00D00000
11D20A3B83445
```

Request URI

SIP Domains (continued)

- From the SMGR web console select the Routing menu.



Avaya Aura® System Manager 6.2

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

UCM Roles
Manage UCM Roles, assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway configurations

Communication Manager
Manage Communication Manager objects

Conferencing
Manage Conferencing Multimedia Server objects

Inventory
Manage, discover, and navigate to elements, update element software

Meeting Exchange
Meeting Exchange

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

Scheduler
Schedule, track, cancel, update and delete jobs

Security
Manage Security Certificates

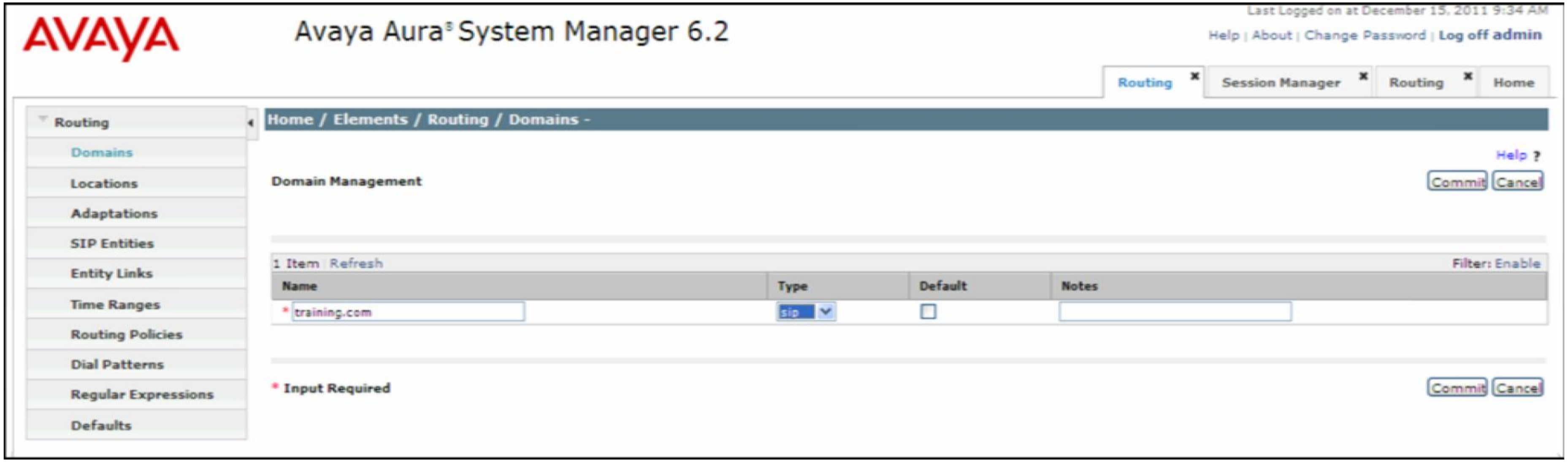
Templates
Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway objects

UCM Services
Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

SIP Domains (continued)

Only Domains of type **SIP** can be used for routing

Routing >> Domains



Domain Management

1 Item | Refresh

Filter: Enable

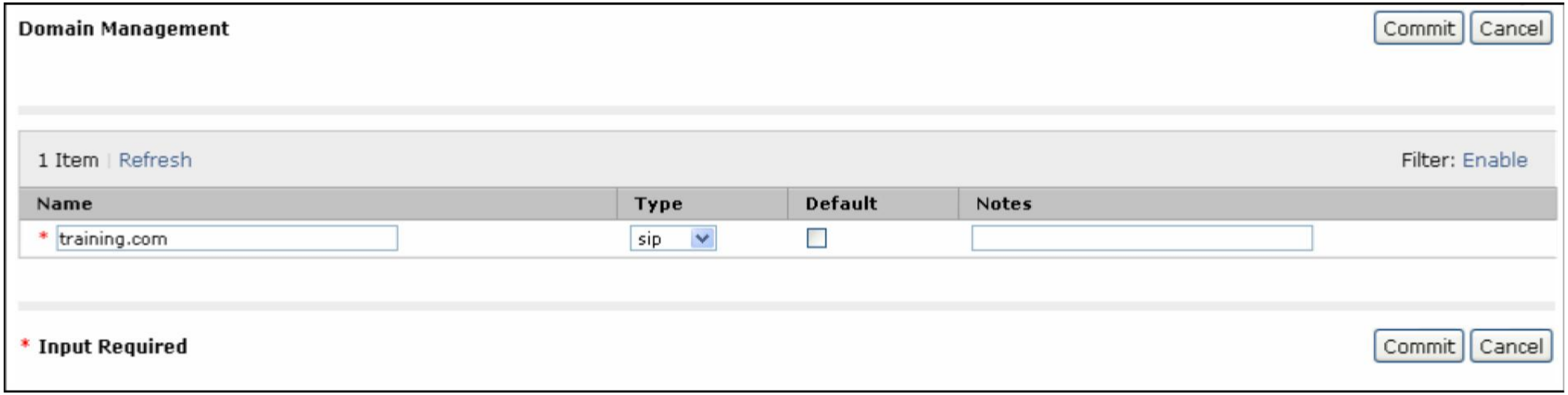
Name	Type	Default	Notes
* training.com	sip	□	

* Input Required

- Select the **Domains** menu.

Exercise: Define a SIP Domain

Step	Action
1	Navigate from the System Manager Home page to Routing Menu >> Domains
2	Student a: define **training.com** as a domain Student b: define **abc.com** as a domain
3	Type: **SIP**
4	Select ***Commit***



Domain Management

1 Item | Refresh

Filter: Enable

Name	Type	Default	Notes
* training.com	sip	□	

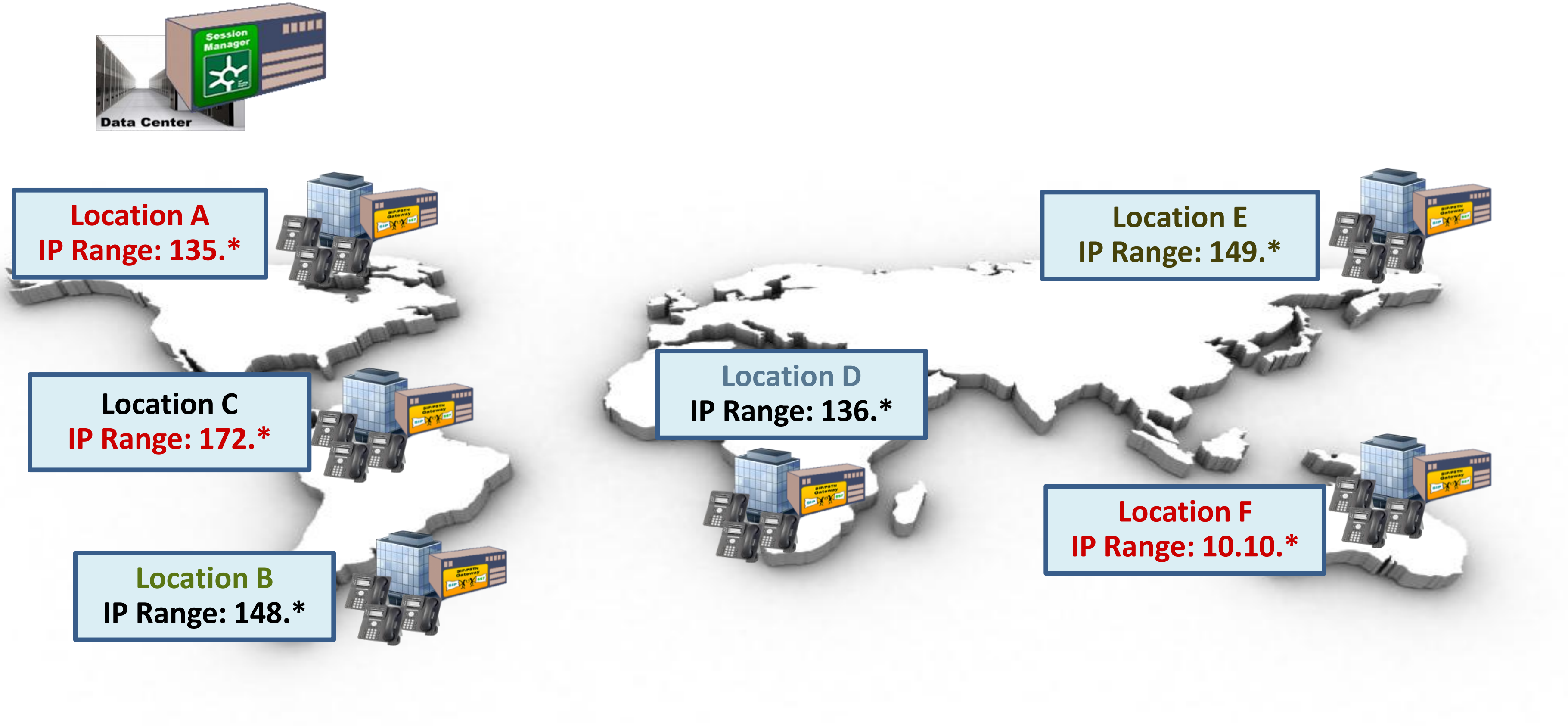
* **Input Required**

Locations

Network Locations

Location is used for:

- Managing the bandwidth to/from or within a location based on CAC settings
- Determining where to send emergency calls (e911)
- Fetching location-specific registration or subscription parameters



Location A
IP Range: 135.*

Location E
IP Range: 149.*

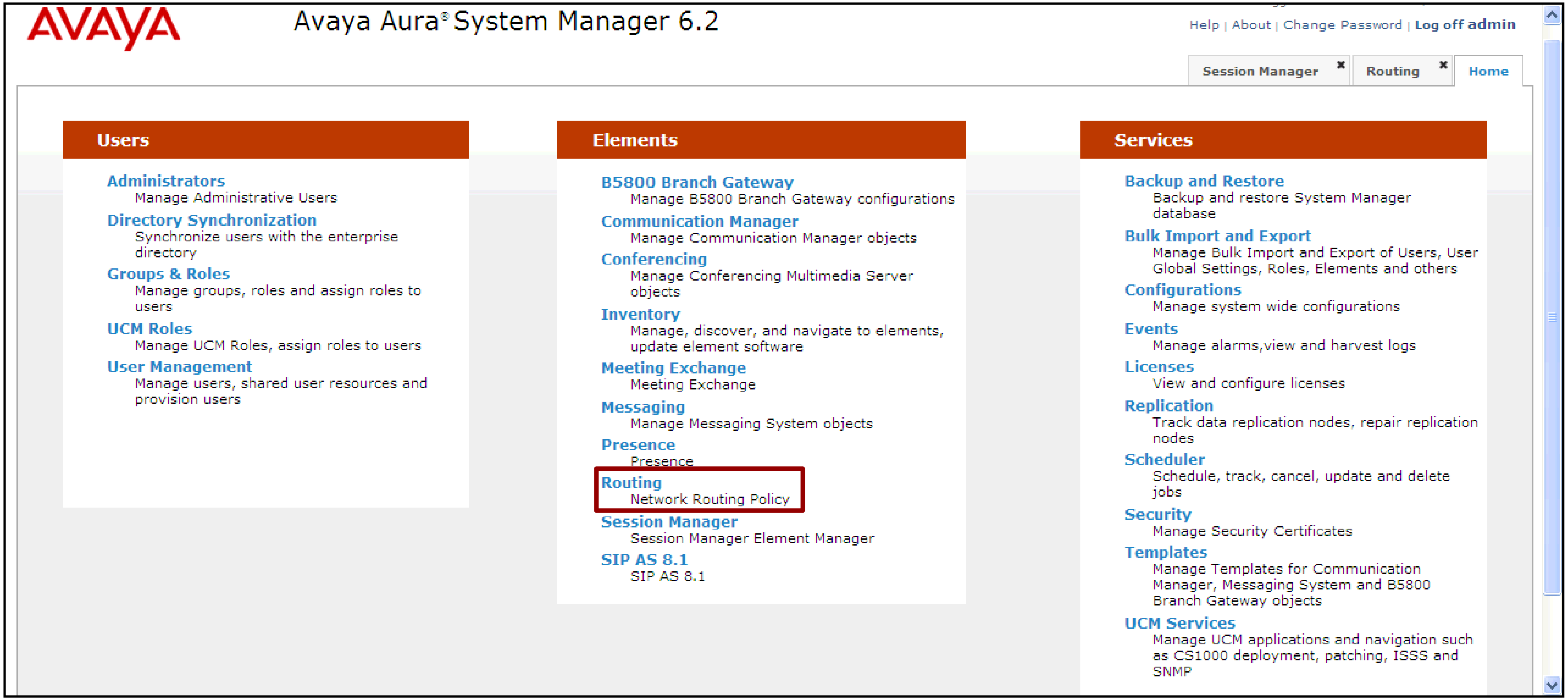
Location C
IP Range: 172.*

Location D
IP Range: 136.*

Location F
IP Range: 10.10.*

Location B
IP Range: 148.*

Locations



AVAYA
Avaya Aura® System Manager 6.2
Help | About | Change Password | Log off admin
Session Manager
Routing
Home

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

UCM Roles
Manage UCM Roles, assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway configurations

Communication Manager
Manage Communication Manager objects

Conferencing
Manage Conferencing Multimedia Server objects

Inventory
Manage, discover, and navigate to elements, update element software

Meeting Exchange
Meeting Exchange

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

Scheduler
Schedule, track, cancel, update and delete jobs

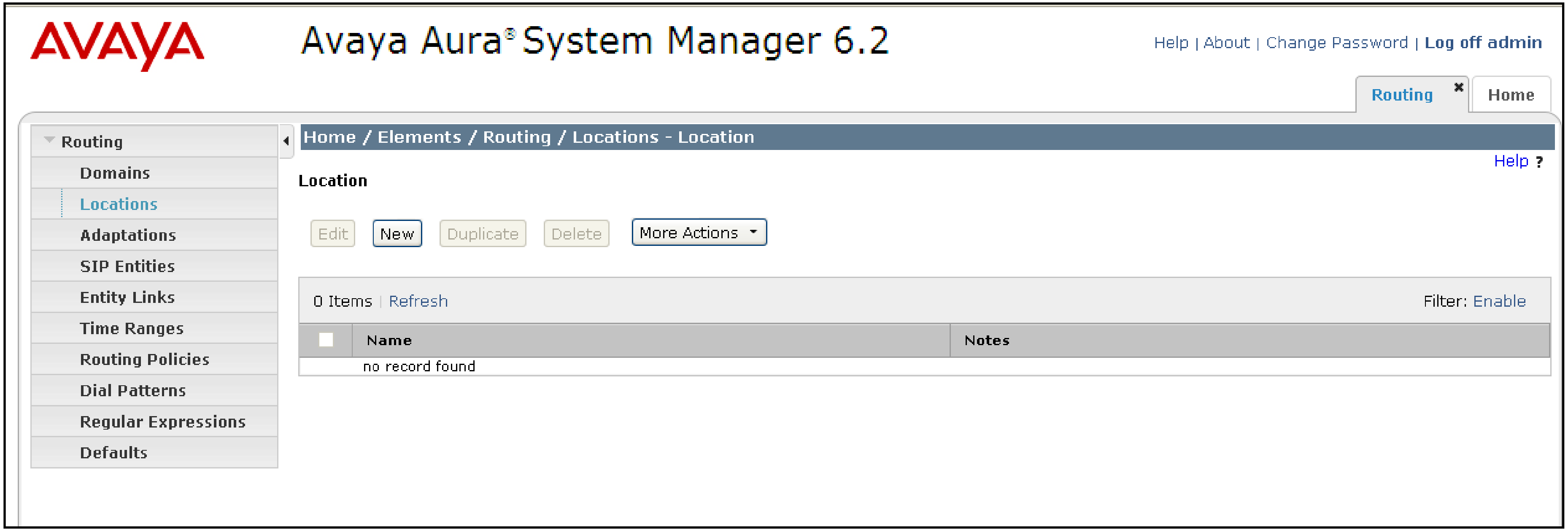
Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway objects

UCM Services
Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

Locations (continued)

Routing >> Locations

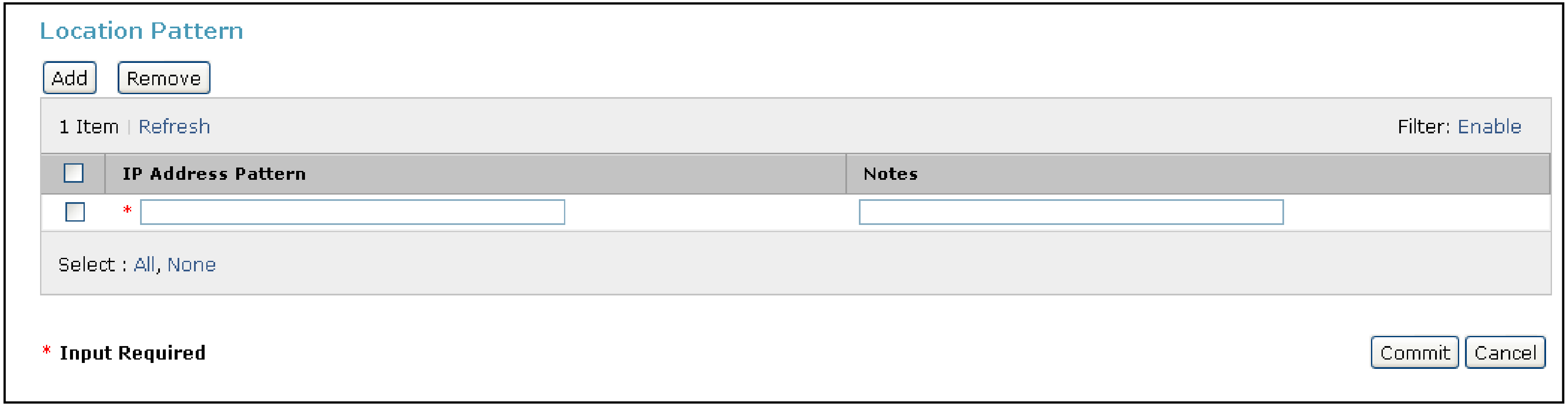


□	Name	Notes
	no record found	

The Location associates an IP address pattern with a name to be used in the Routing Policy to determine the originating location of a call.

Locations (continued)

The Locations screen can contain one or several IP addresses. Each SIP entity has a particular IP address.



□	IP Address Pattern	Notes
□	*	

* Input Required

Examples of IP Address Patterns:

172.*

172.16x.121.123

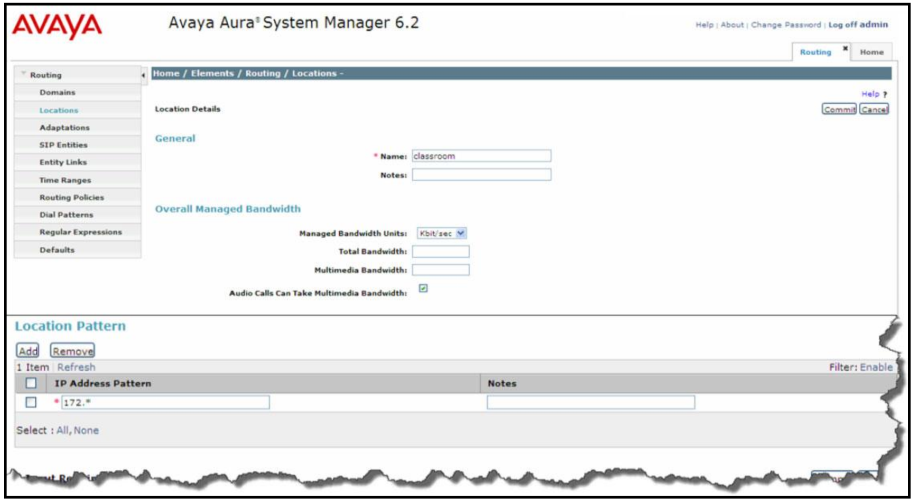
172.16x.121.*

10.0.0.1-10.0.0.5

135.9.0.0/16

Exercise: Create a Location in the SIP Domain

Step	Action
1	Navigate from Routing Menu >> Locations
2	Create a new Location : Student a:create **Denver** location Student b:create **Basking Ridge** location
3	Scroll down to Location Pattern Select Add IP Address pattern : Denver **172.*** Basking Ridge **135.***
4	Select ***Commit***



Location Details

General

* Name: classroom

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☑

Location Pattern

☐	IP Address Pattern	Notes
☐	* 172.*	

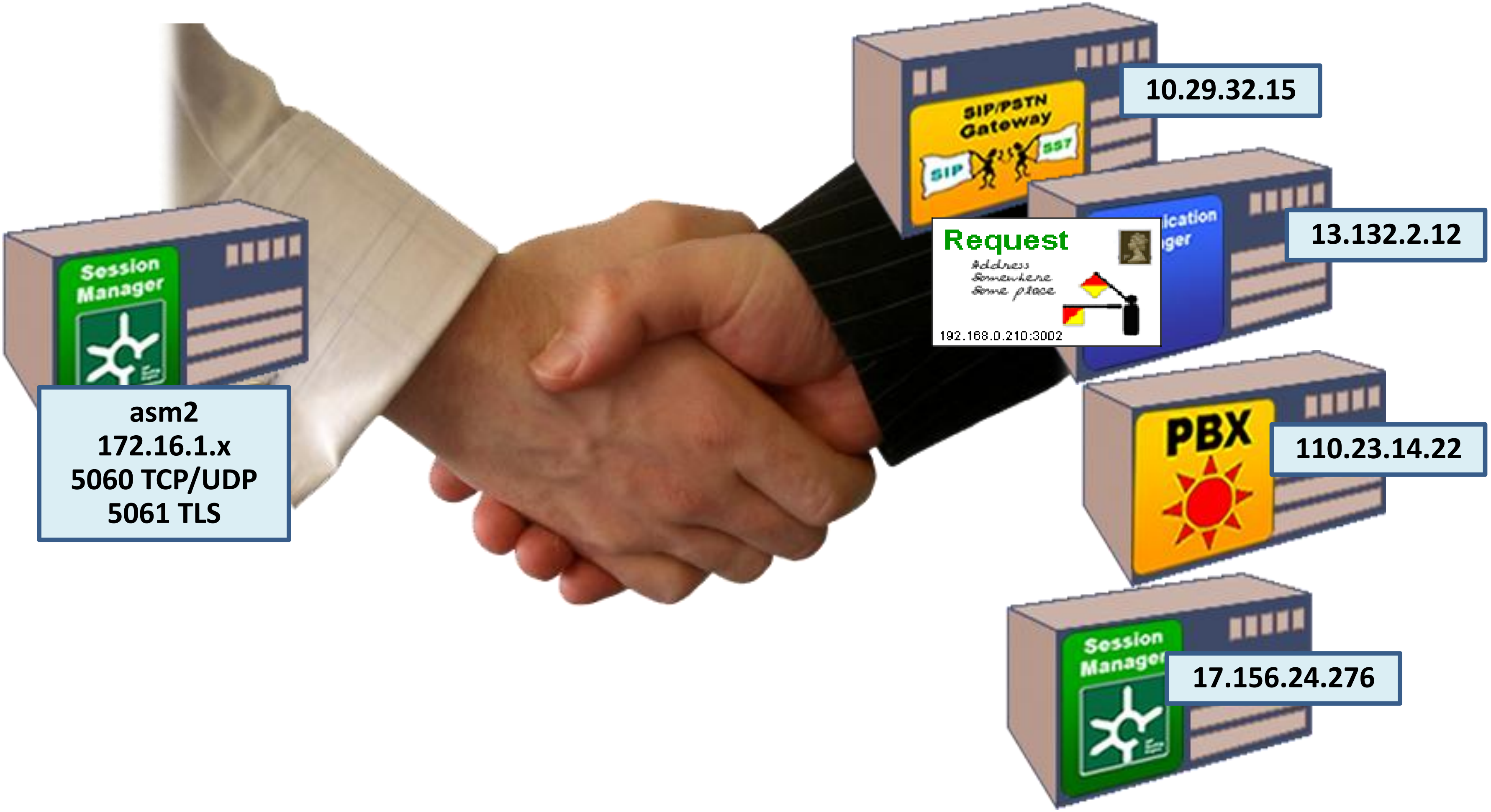
Select : All, None

AVAYA | LEARNING

SIP Entities

Trusted SIP Entities

- Session Manager validates each SIP entity and does not accept connections matching untrusted entity links.



asm2
172.16.1.x
5060 TCP/UDP
5061 TLS

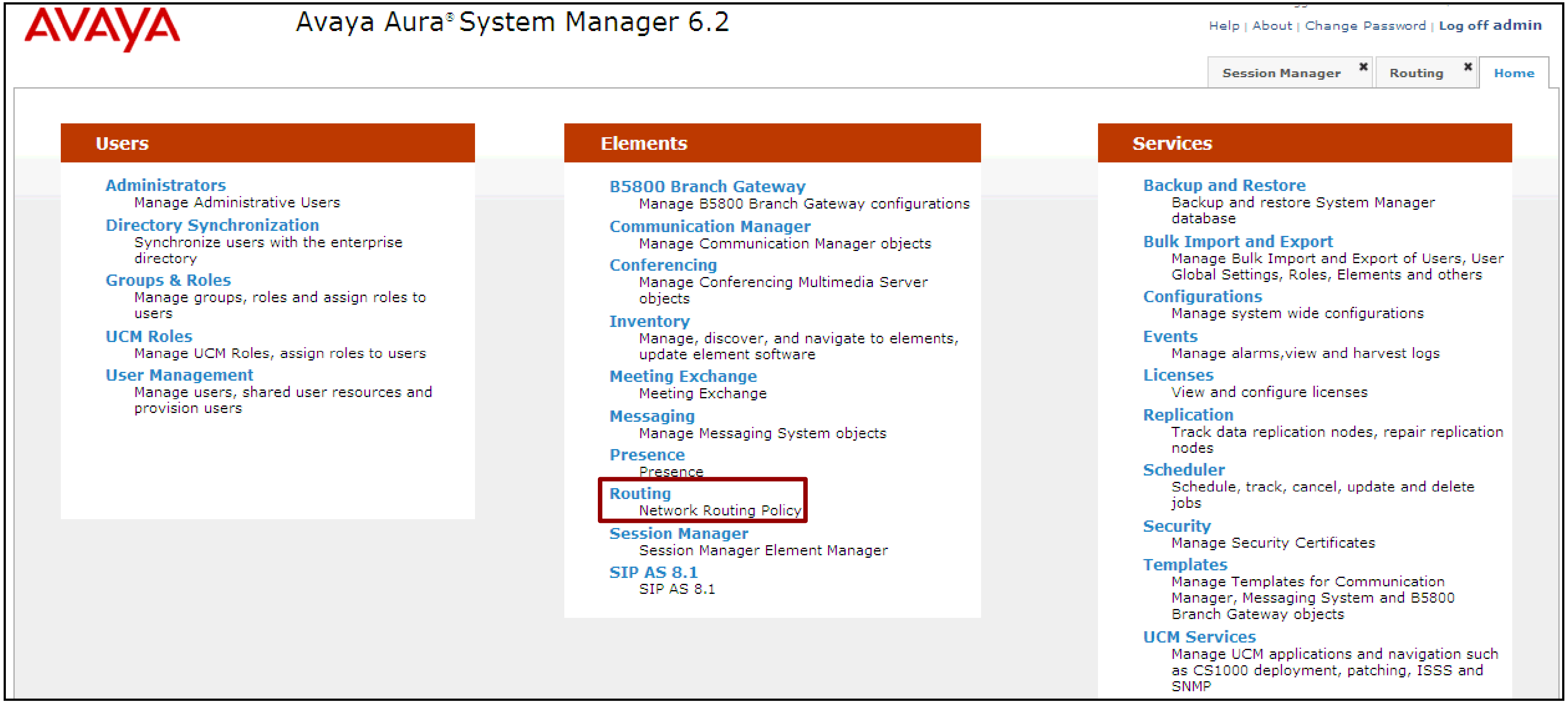
10.29.32.15

13.132.2.12

110.23.14.22

17.156.24.276

SIP Entities



Avaya Aura® System Manager 6.2

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

UCM Roles
Manage UCM Roles, assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway configurations

Communication Manager
Manage Communication Manager objects

Conferencing
Manage Conferencing Multimedia Server objects

Inventory
Manage, discover, and navigate to elements, update element software

Meeting Exchange
Meeting Exchange

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

Scheduler
Schedule, track, cancel, update and delete jobs

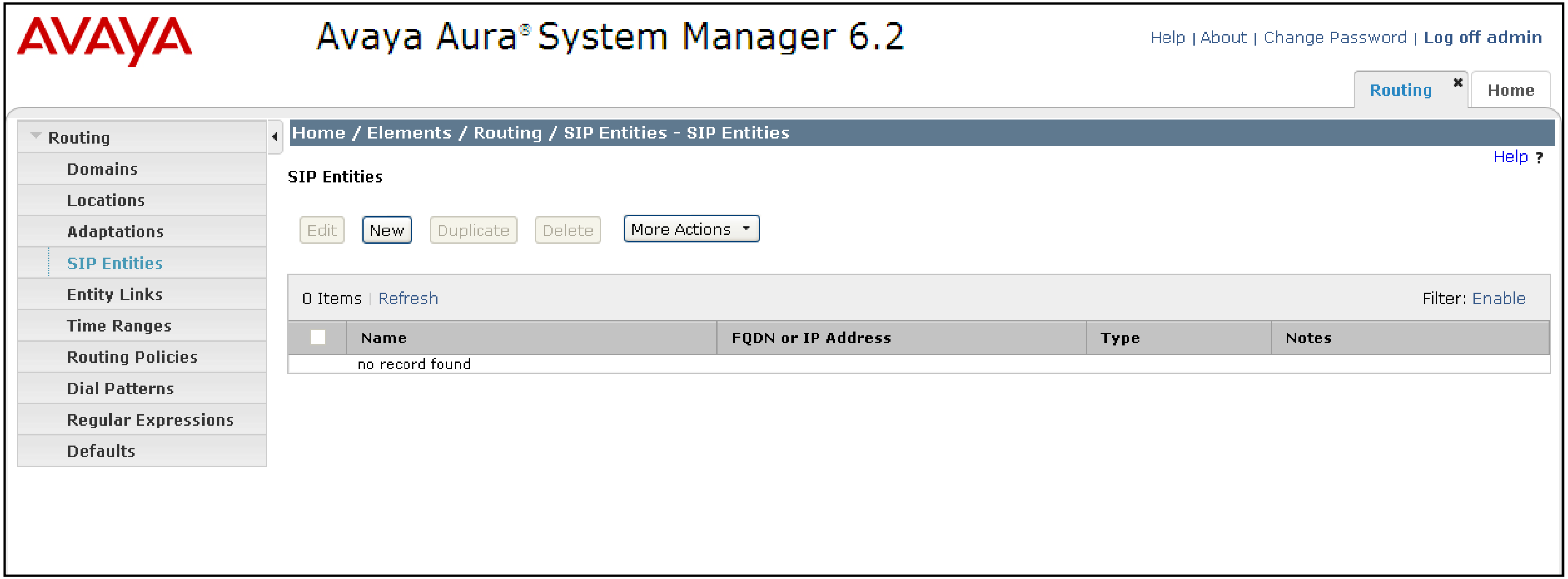
Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway objects

UCM Services
Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

SIP Entities (continued)

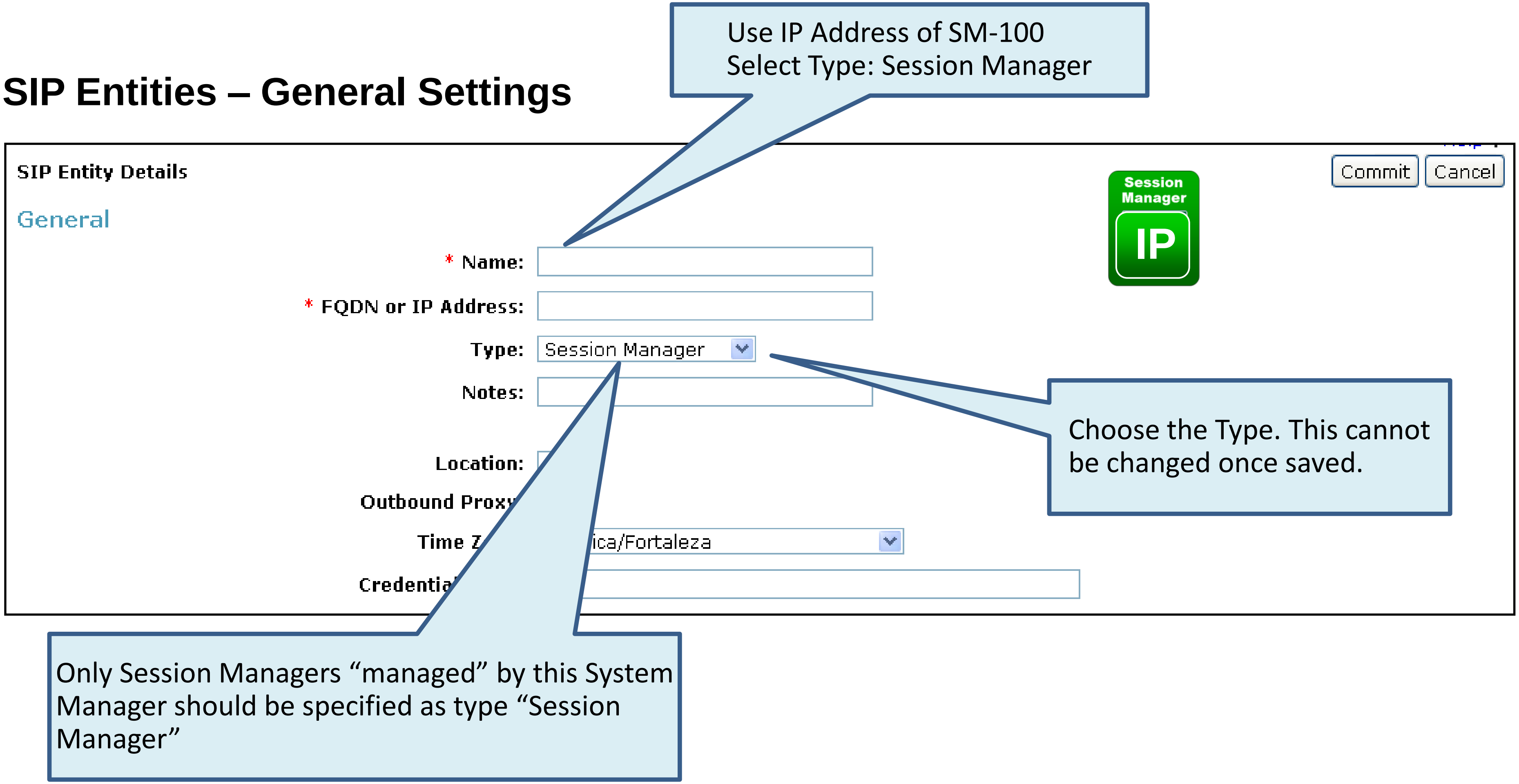
- From the Routing Menu select SIP Entities
- Select New



□	Name	FQDN or IP Address	Type	Notes
	no record found			

SIP Entity – Session Manager

SIP Entities – General Settings



SIP Entity Details

General

* Name:

* FQDN or IP Address:

Type: Session Manager

Notes:

Location:

Outbound Proxy

Time Z ica/Fortaleza

Credentia

Use IP Address of SM-100
Select Type: Session Manager

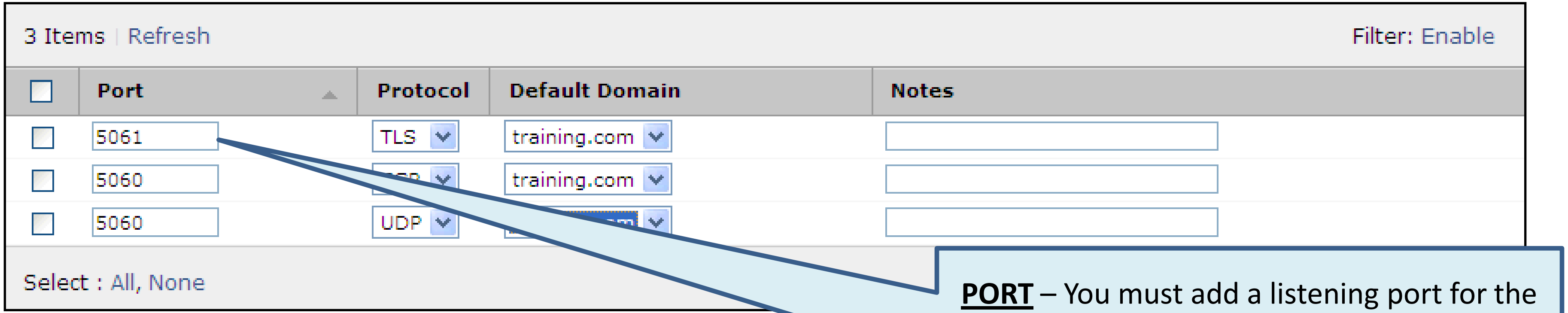
Choose the Type. This cannot be changed once saved.

Only Session Managers “managed” by this System Manager should be specified as type “Session Manager”

- Different fields will appear when adding a SIP entity other than Session Manager. They will be covered later when adding CM.

SIP Entities- Ports

Defines the port(s), transport protocol(s) and default domains on which this Session Manager listens for SIP traffic.



3 Items | Refresh

Filter: Enable

□	Port	Protocol	Default Domain	Notes
□	5061	TLS	training.com	
□	5060	TCP	training.com	
□	5060	UDP	[illegible]	

Select : All, None

PORT – You must add a listening port for the Session Manager SIP Entity.

Add a port for TCP, TLS and UDP.

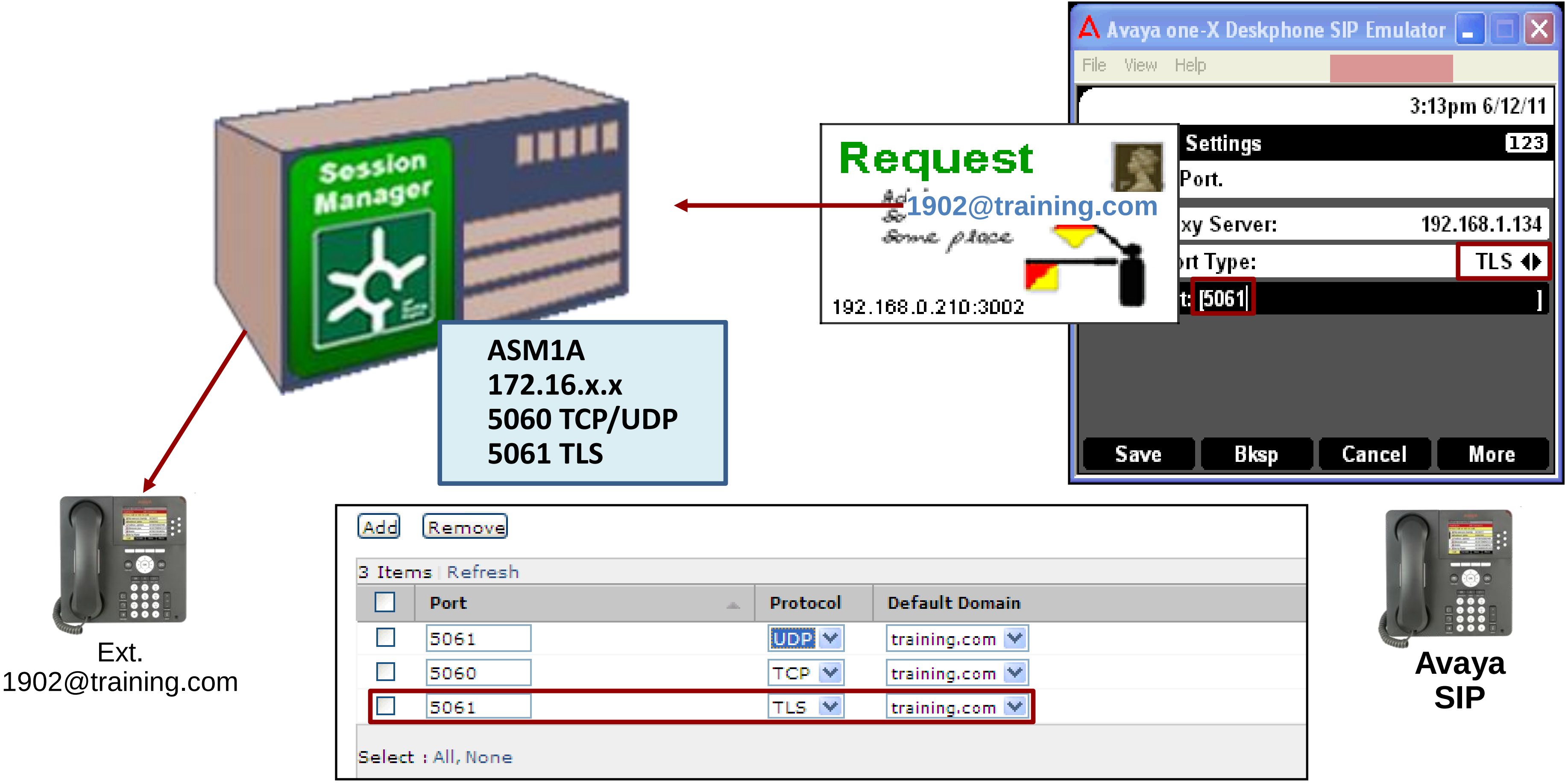
You must specify a Default Domain.

- The Protocols field are transport protocols used for transporting the SIP messages.
- TLS is used for encrypted transport of SIP Messages and is recommended for secure SIP.

SIP Domain Routing

- When Session Manager receives a request, it associates one of the administered domains with the port on which the request was received.

SIP Phone Settings



ASM1A
172.16.x.x
5060 TCP/UDP
5061 TLS

Request
1902@training.com
192.168.0.210:3002

Avaya one-X Deskphone SIP Emulator

3:13pm 6/12/11

Settings 123

Port.

xy Server: 192.168.1.134

rt Type: TLS

t: [5061]

Ext.
1902@training.com

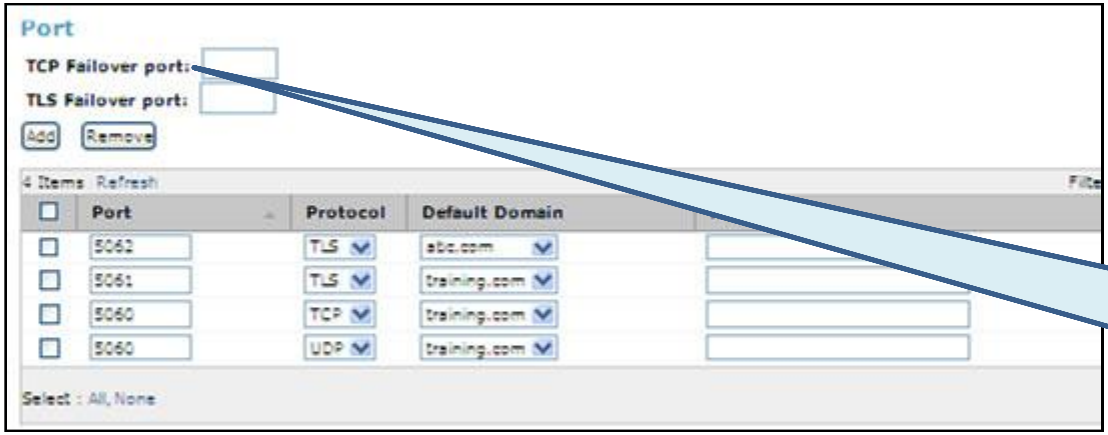
Avaya
SIP

3 Items | Refresh

□	Port	Protocol	Default Domain
□	5061	UDP	training.com
□	5060	TCP	training.com
□	5061	TLS	training.com

Select : All, None

Failover Ports



Port

TCP Failover port:

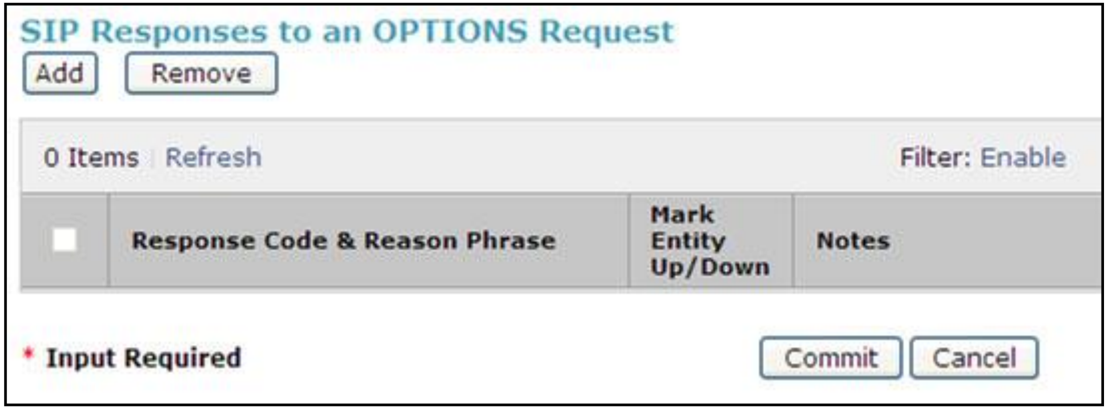
TLS Failover port:

Add Remove

4 Items Refresh

□	Port	Protocol	Default Domain	
□	5062	TLS	abc.com	
□	5061	TLS	training.com	
□	5060	TCP	training.com	
□	5060	UDP	training.com	

Select : All, None



SIP Responses to an OPTIONS Request

Add Remove

0 Items Refresh Filter: Enable

□	Response Code & Reason Phrase	Mark Entity Up/Down	Notes

* Input Required

Commit Cancel

FAILOVER PORT – Add Failover ports if the SIP entity is a failover group member.

Exercise: Define your Session Manager SIP Entity

Step	Action
1	Name your Session Manager SIP Entity: For Example **ASM1, ASM2, ASM3, ASM4, ASM5, ASM6**
2	Use the IP Address of your Security Module ETH2: **172.16.x.105** Check the Classroom Layout document for reference
3	Type is "**Session Manager**"
4	Location is "**Denver**'
5	Select Time zone **America/Denver**
6	Add 4 Ports: **5061 TLS training.com** **5060 TCP training.com** **5060 UDP training.com** **5063 TLS abc.com**

Session Manager Instance

Session Manager Instance

Master DB

Data Repository
Database

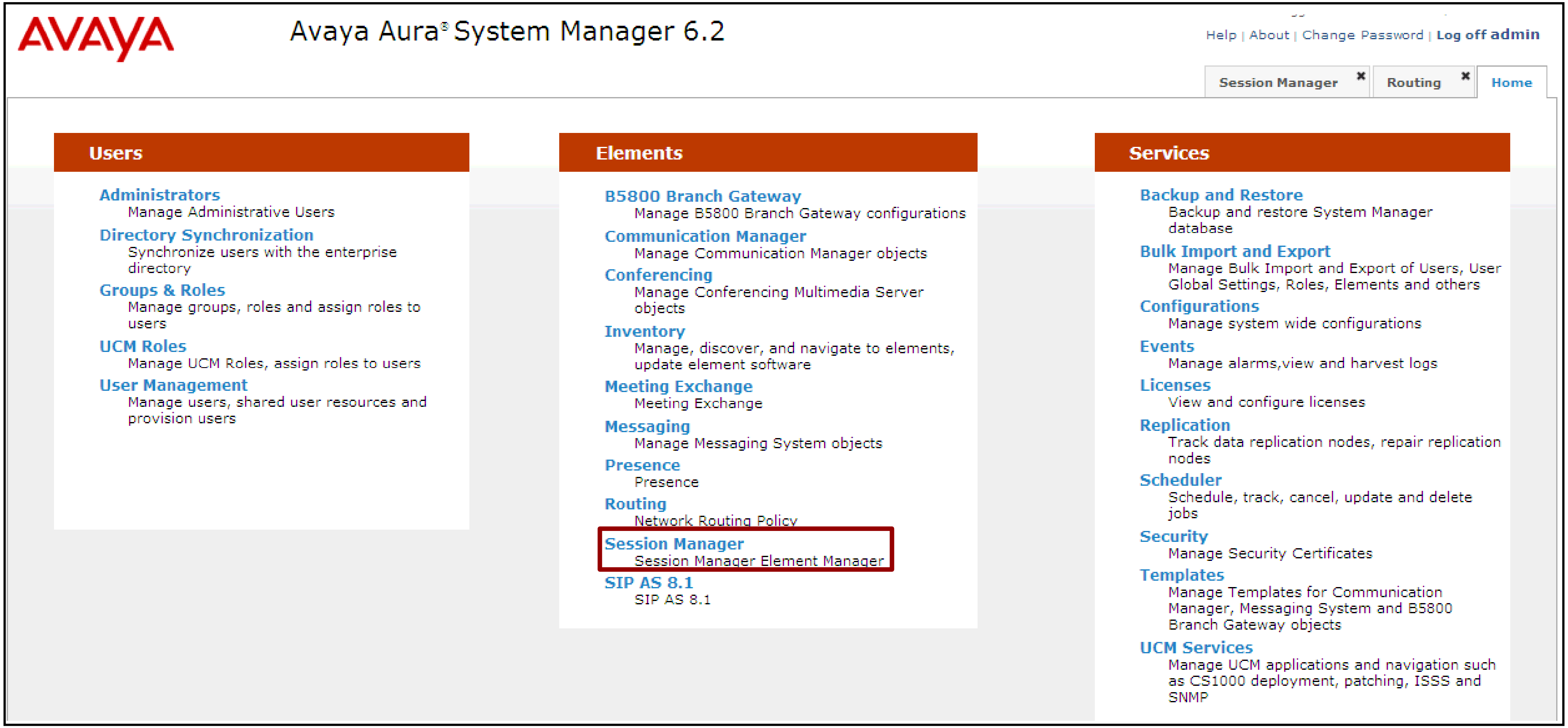
Replica DB

Data Repository
Database

Only after a Session manager Instance is defined can we:

- Monitor health and status of the Session Manager
- Administer Routing Policies, User’s Communication Profiles and Application Sequencing

Session Manager Instance (continued)



Avaya Aura® System Manager 6.2

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

UCM Roles
Manage UCM Roles, assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway configurations

Communication Manager
Manage Communication Manager objects

Conferencing
Manage Conferencing Multimedia Server objects

Inventory
Manage, discover, and navigate to elements, update element software

Meeting Exchange
Meeting Exchange

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

Scheduler
Schedule, track, cancel, update and delete jobs

Security
Manage Security Certificates

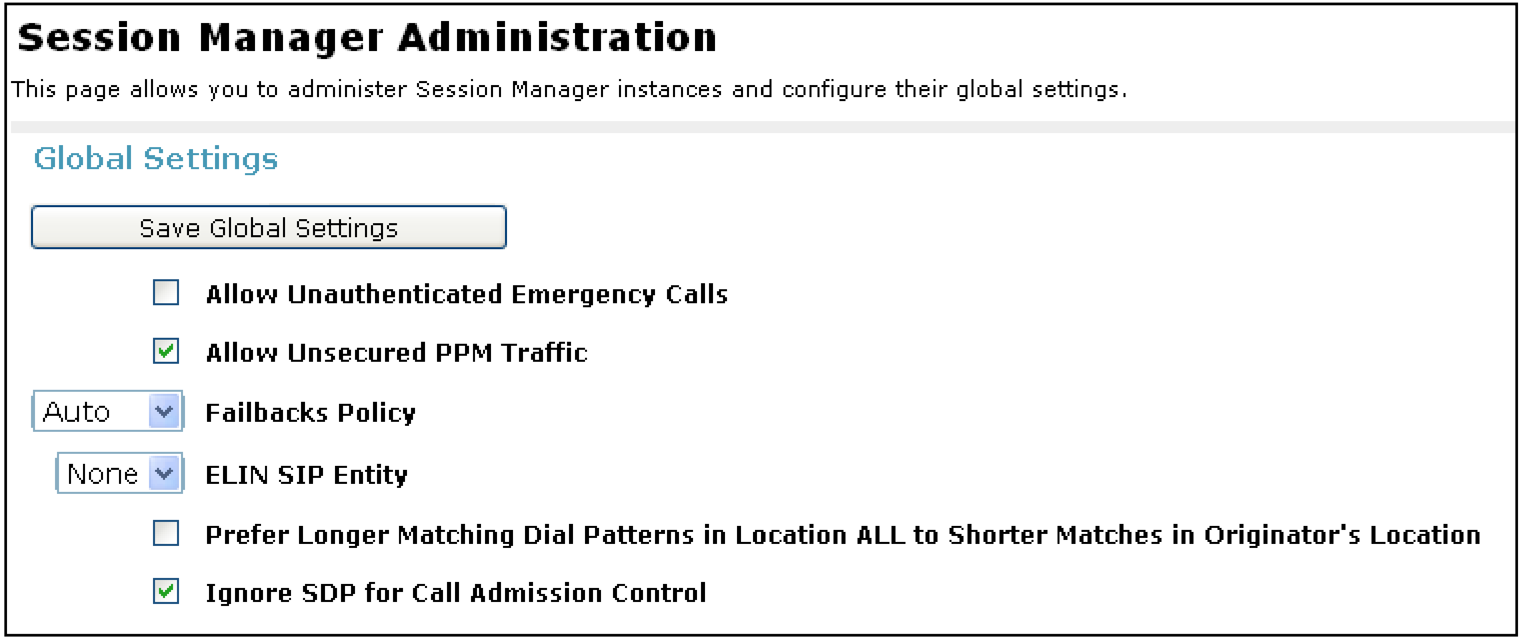
Templates
Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway objects

UCM Services
Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

Session Manager Instance (continued)

Global Settings:

- Deselect Ignore SDP for Call Admission Control
- All other settings leave as default



Session Manager Administration

This page allows you to administer Session Manager instances and configure their global settings.

Global Settings

☐ Allow Unauthenticated Emergency Calls

☑ Allow Unsecured PPM Traffic

Auto Failbacks Policy

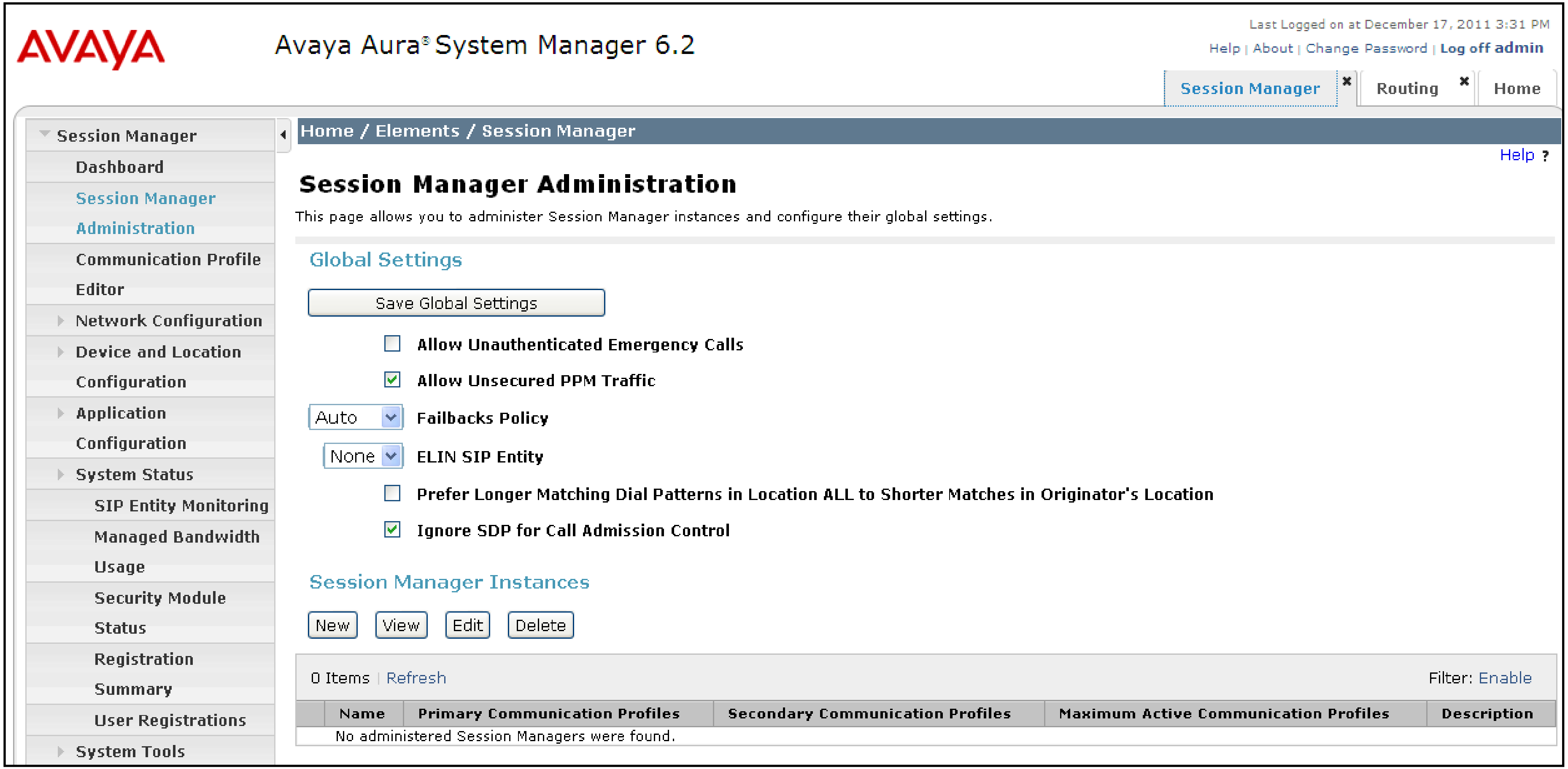
None ELIN SIP Entity

☐ Prefer Longer Matching Dial Patterns in Location ALL to Shorter Matches in Originator's Location

☑ Ignore SDP for Call Admission Control

Session Manager Instance (continued)

Session Manager >> Session Manager Administration >> Select New



AVAYA
Avaya Aura® System Manager 6.2
Last Logged on at December 17, 2011 3:31 PM
Help | About | Change Password | Log off admin
Session Manager
Routing
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
SIP Entity Monitoring
Managed Bandwidth Usage
Security Module Status
Registration Summary
User Registrations
System Tools
Home / Elements / Session Manager
Help ?

Session Manager Administration

This page allows you to administer Session Manager instances and configure their global settings.

Global Settings

Save Global Settings

□ Allow Unauthenticated Emergency Calls

☑ Allow Unsecured PPM Traffic

Auto Failbacks Policy

None ELIN SIP Entity

□ Prefer Longer Matching Dial Patterns in Location ALL to Shorter Matches in Originator's Location

☑ Ignore SDP for Call Admission Control

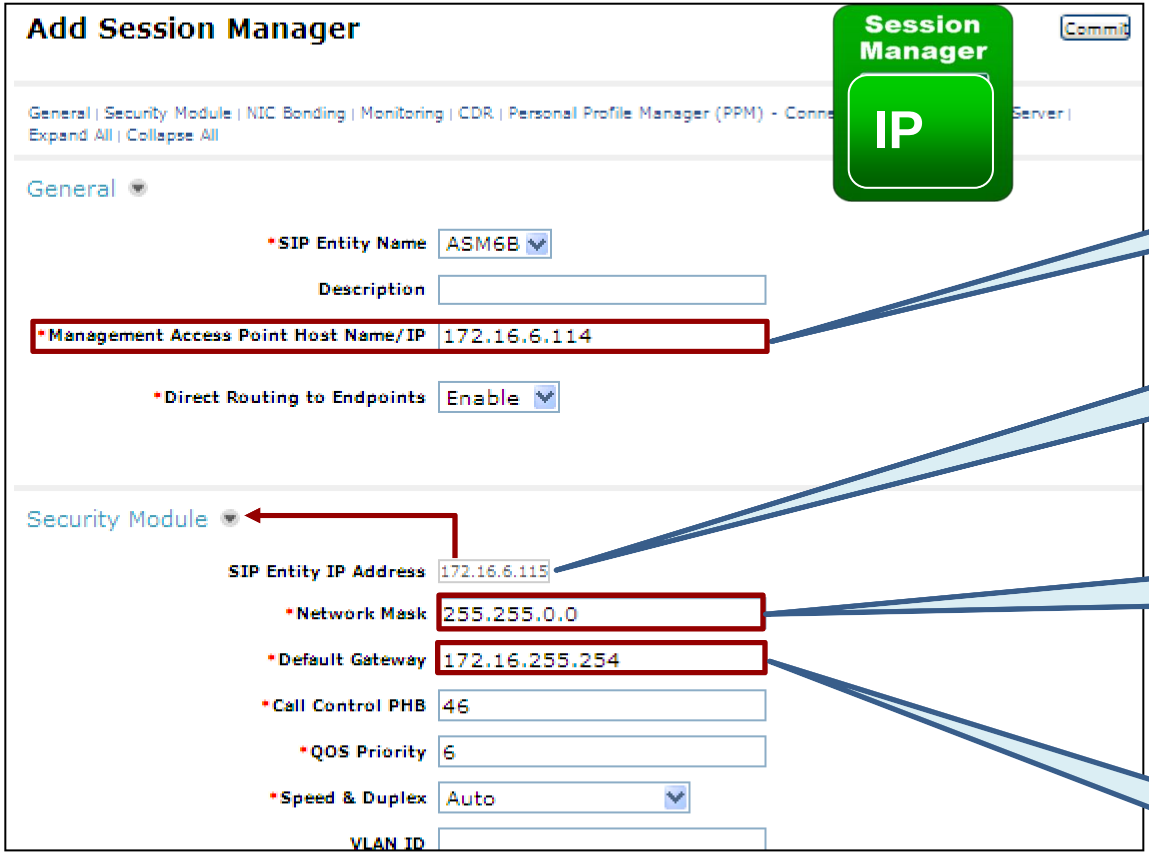
Session Manager Instances

New | View | Edit | Delete

0 Items | Refresh — Filter: Enable

	Name	Primary Communication Profiles	Secondary Communication Profiles	Maximum Active Communication Profiles	Description
	No administered Session Managers were found.				

Define Session Manager Instance (continued)



Add Session Manager

Session Manager
IP
Commit
General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Conn
Server |
Expand All | Collapse All

General

*SIP Entity Name	ASM6B
Description	
*Management Access Point Host Name/IP	172.16.6.114
*Direct Routing to Endpoints	Enable

Security Module

SIP Entity IP Address	172.16.6.115
*Network Mask	255.255.0.0
*Default Gateway	172.16.255.254
*Call Control PHB	46
*QOS Priority	6
*Speed & Duplex	Auto
VLAN ID	

IP Address of Session Manager's eth0

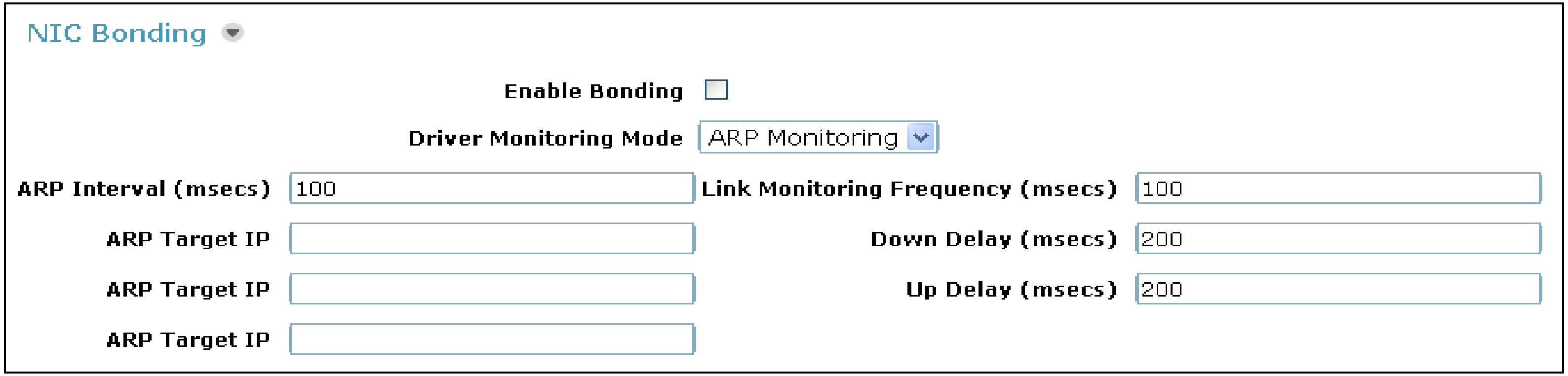
Defaults based on IP Address defined in SIP Entity

Enter subnet mask: 255.255.0.0

Enter Default Gateway: 172.16.255.254

Session Manager Instance (continued)

- For added high availability, NIC Bonding can be configured.
- This bonds interfaces ETH2 and ETH3 and makes all network firewall capability applicable to ETH3.



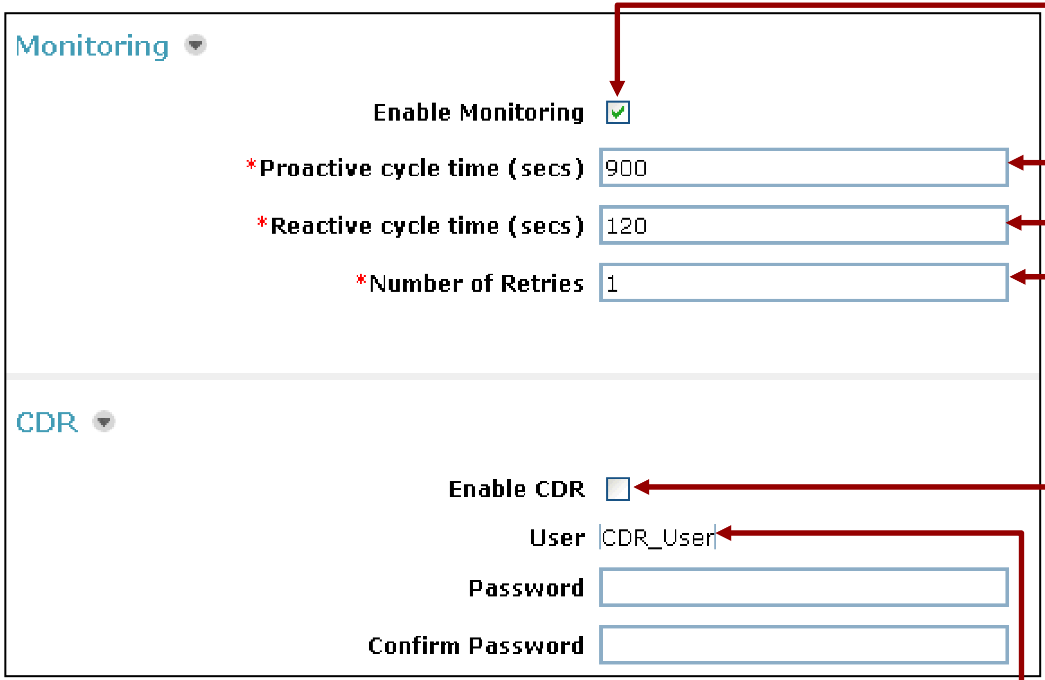
NIC Bonding

Enable Bonding □

Driver Monitoring Mode: ARP Monitoring

ARP Interval (msecs)	100	Link Monitoring Frequency (msecs)	100
ARP Target IP		Down Delay (msecs)	200
ARP Target IP		Up Delay (msecs)	200
ARP Target IP			

Session Manager Instance (continued)



Monitoring

Enable Monitoring ☑

*Proactive cycle time (secs) 900

*Reactive cycle time (secs) 120

*Number of Retries 1

CDR

Enable CDR □

User CDR_User

Password

Confirm Password

To enable or disable monitoring of the SIP entities by this Session Manage instance

How often the entity is monitored when the link to the entity is up or active

How often the entity is monitored when a link to the entity is down or inactive

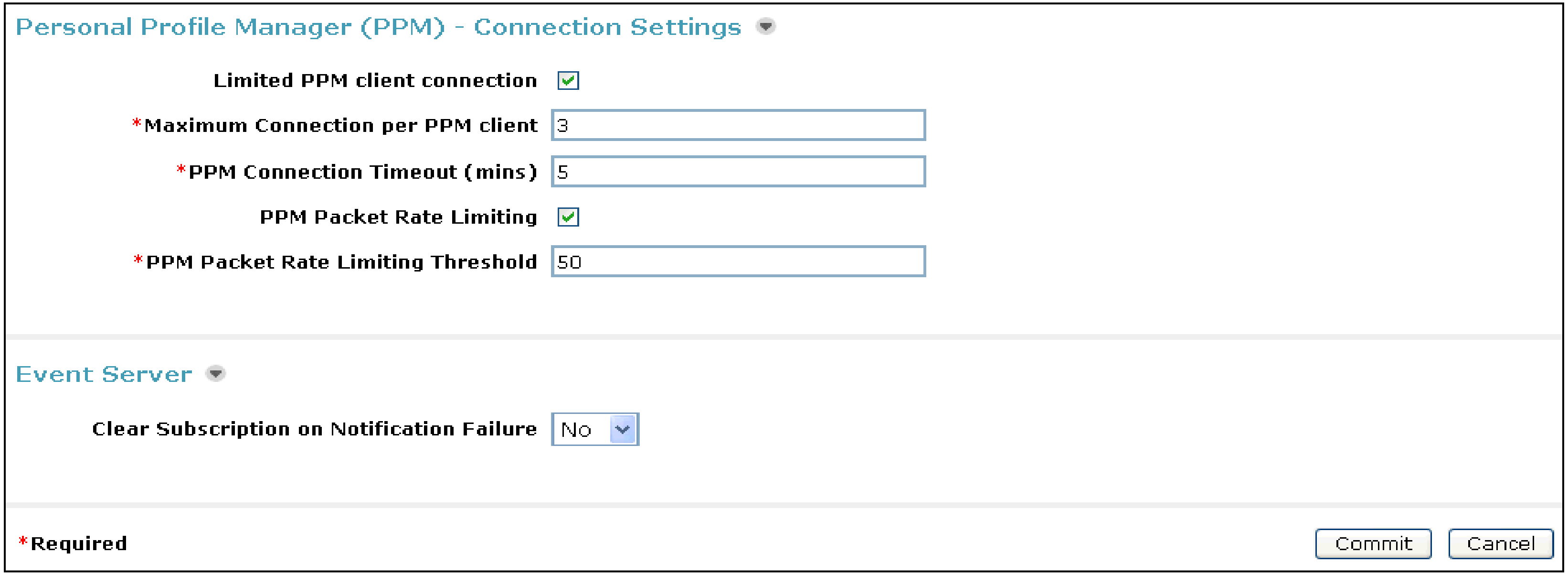
The number of times Session Manager tries to reach the SIP entity before marking it as down or unavailable

This controls whether CDR is enabled at the system level for that Session Manager instance.

If CDR is enabled, you can individually control call detail recording for specific SIP entities using the Call Detail Recording drop-down menu.

Define Session Manager (continued)

- PPM Connection settings specify the global parameters that apply to all SM instances.
- Limits the number of connections per endpoint to the PPM service in Session Manager.
- More on PPM in the next module.



Personal Profile Manager (PPM) - Connection Settings

Limited PPM client connection ☑

*Maximum Connection per PPM client: 3

*PPM Connection Timeout (mins): 5

PPM Packet Rate Limiting ☑

*PPM Packet Rate Limiting Threshold: 50

Event Server

Clear Subscription on Notification Failure: No

*Required

Exercise: Define a Session Manager Instance

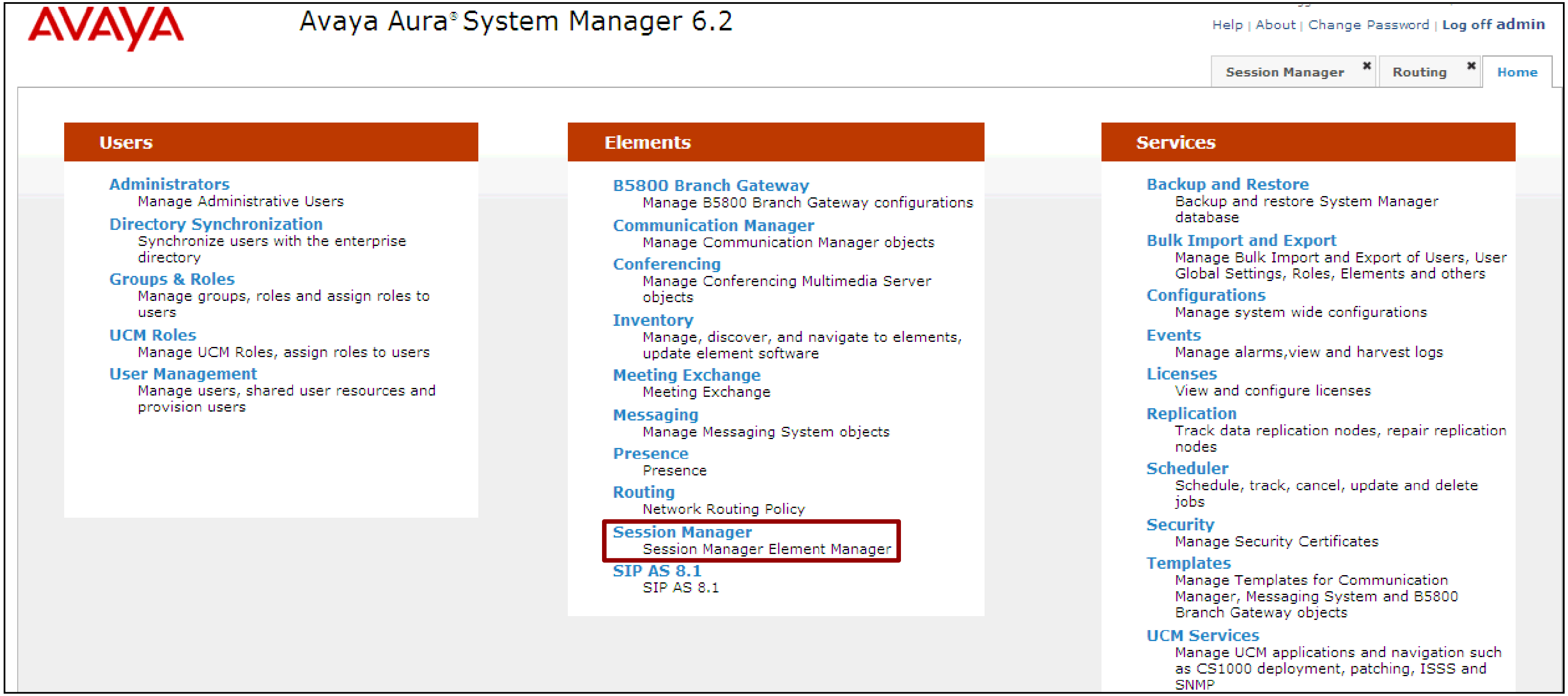
- Make note of the correct IP addresses used in the Session Manager Instance.
- Eth0: 172.16.x.104
- Eth2: 172.16.x.105

Step	Action
1	Navigate to Elements Column >> Session Manager Administration
2	Define the *Session Manager Instance* Select New
3	Enter the following data: ● *Select the SIP Entity you previously defined in the SIP Entity Name drop-down list* ● *The management address for* ***<u>Session Manager</u>*** (ETH0: **172.16.x.104**) ● The Netmask = **255.255.0.0** ● The Gateway = **172.16.255.254** ● *Let all other fields default*
4	***Commit***

AVAYA | LEARNING

Post Configuration Checks

Post Configuration



Avaya Aura® System Manager 6.2

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

UCM Roles
Manage UCM Roles, assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway configurations

Communication Manager
Manage Communication Manager objects

Conferencing
Manage Conferencing Multimedia Server objects

Inventory
Manage, discover, and navigate to elements, update element software

Meeting Exchange
Meeting Exchange

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

Scheduler
Schedule, track, cancel, update and delete jobs

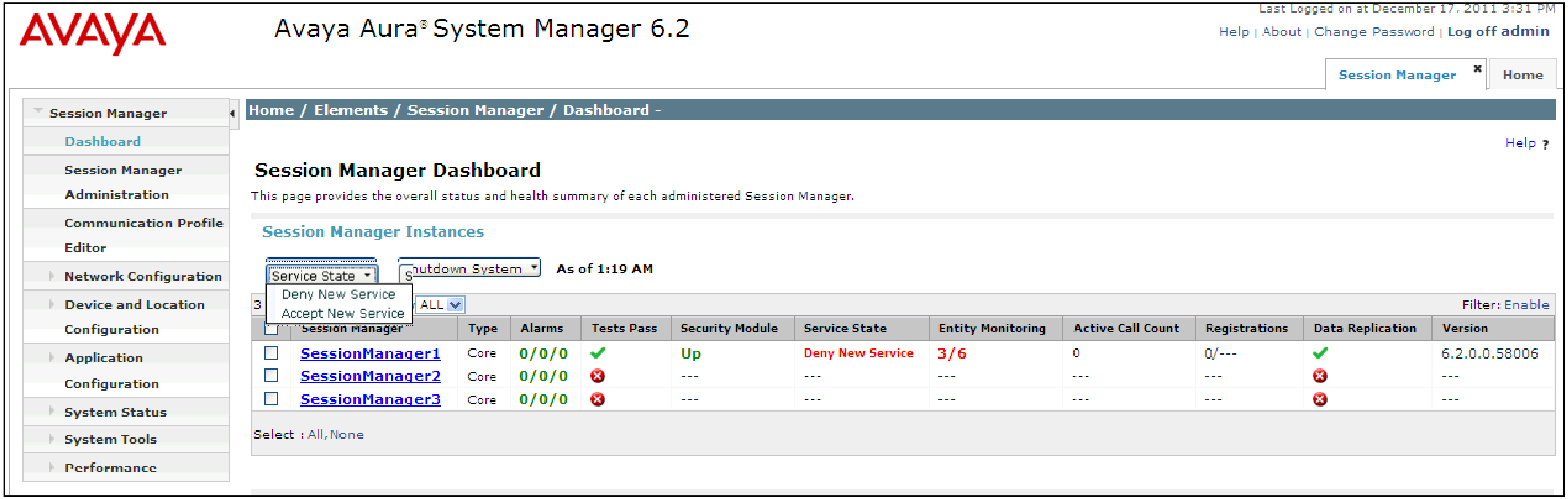
Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway objects

UCM Services
Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

Enable New Service

- Just like a SIP Firewall is by default not configured to accept traffic, the SM100 Security Module must be enabled before it can begin to receive SIP traffic.
- The default state of the Session Manager is *Deny New Service* so it must be enabled to start the SM-100 and take calls.



AVAYA Avaya Aura® System Manager 6.2

Last Logged on at December 17, 2011 3:31 PM

Help | About | Change Password | Log off admin

Session Manager
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Performance
Home / Elements / Session Manager / Dashboard -
Help ?

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

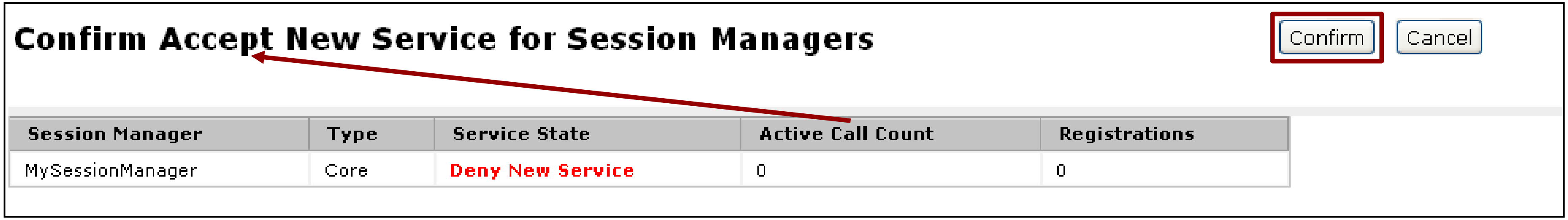
Session Manager Instances

As of 1:19 AM

Filter: Enable

□	Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	Version
□	SessionManager1	Core	0/0/0	✓	Up	Deny New Service	3/6	0	0/---	✓	6.2.0.0.58006
□	SessionManager2	Core	0/0/0	✗	---	---	---	---	---	✗	---
□	SessionManager3	Core	0/0/0	✗	---	---	---	---	---	✗	---

Select : All, None

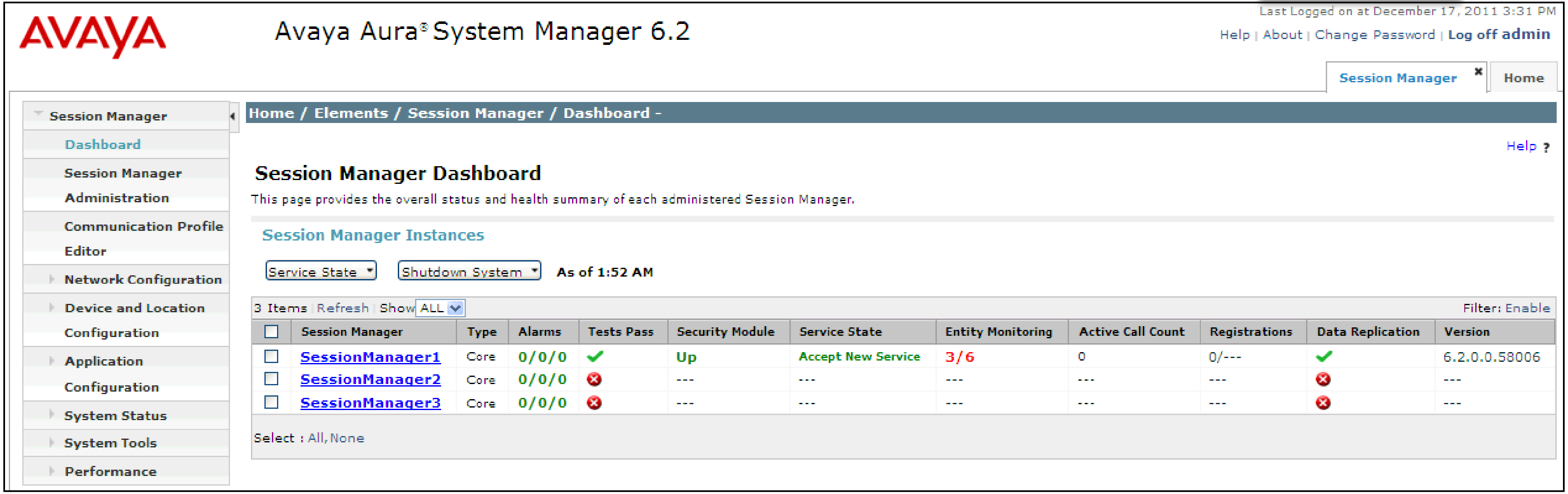


Confirm Accept New Service for Session Managers

Session Manager	Type	Service State	Active Call Count	Registrations
MySessionManager	Core	Deny New Service	0	0

Monitor Session Manager Status

- Session Manager SM100 Module Service State is **Accept New Service** and it is activated and ready for SIP Service.



AVAYA
Avaya Aura® System Manager 6.2
Last Logged on at December 17, 2011 3:31 PM
Help | About | Change Password | Log off admin
Session Manager
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Performance
Home / Elements / Session Manager / Dashboard -
Help ?

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State ▾ Shutdown System ▾ As of 1:52 AM

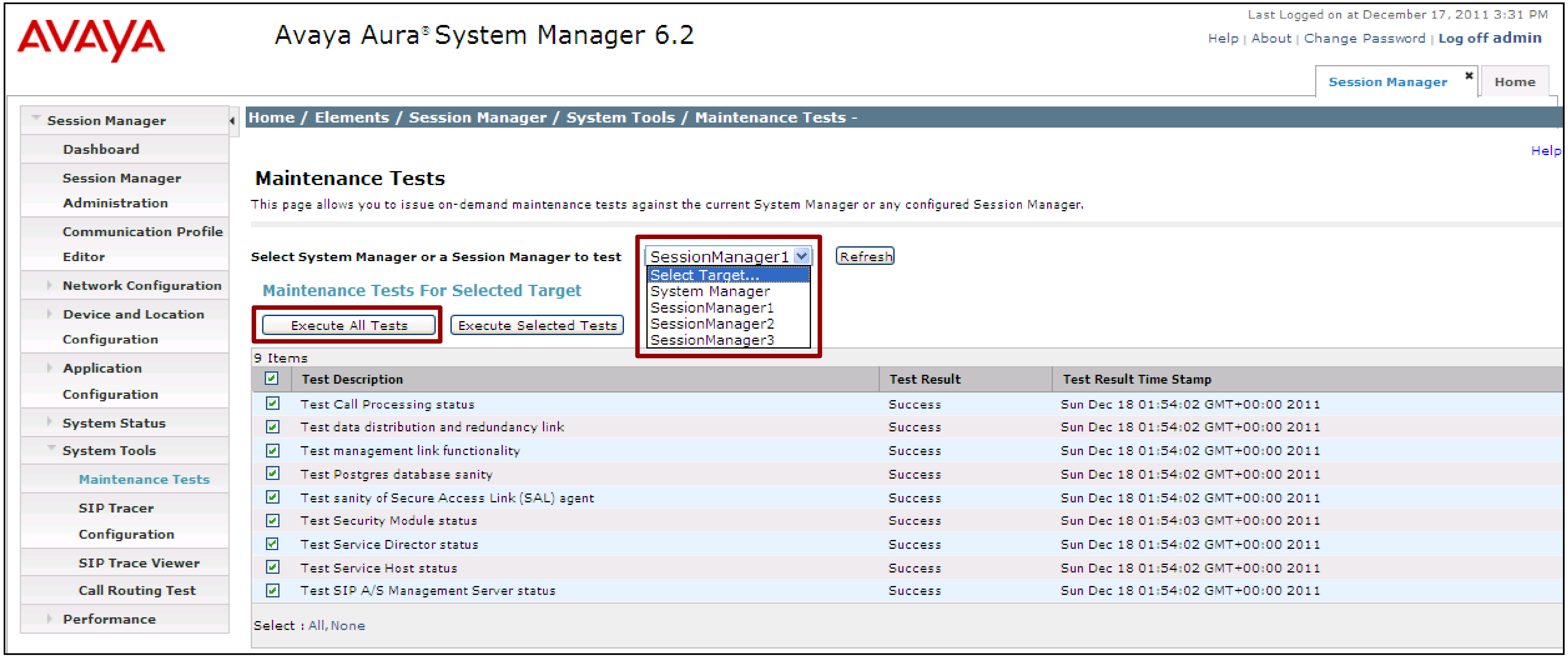
3 Items | Refresh | Show ALL ▾ Filter: Enable

□	Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	Version
□	SessionManager1	Core	0/0/0	✓	Up	Accept New Service	3/6	0	0/---	✓	6.2.0.0.58006
□	SessionManager2	Core	0/0/0	✗	---	---	---	---	---	✗	---
□	SessionManager3	Core	0/0/0	✗	---	---	---	---	---	✗	---

Select : All, None

Maintenance Tests

- Useful for baselining Session and System Manager after an installation.



AVAYA
Avaya Aura® System Manager 6.2
Last Logged on at December 17, 2011 3:31 PM
Help | About | Change Password | Log off admin
Session Manager
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Maintenance Tests
SIP Tracer Configuration
SIP Trace Viewer
Call Routing Test
Performance
Home / Elements / Session Manager / System Tools / Maintenance Tests -
Help

Maintenance Tests

This page allows you to issue on-demand maintenance tests against the current System Manager or any configured Session Manager.

Select System Manager or a Session Manager to test: SessionManager1 (Select Target..., System Manager, SessionManager1, SessionManager2, SessionManager3) Refresh

Maintenance Tests For Selected Target

Execute All Tests | Execute Selected Tests

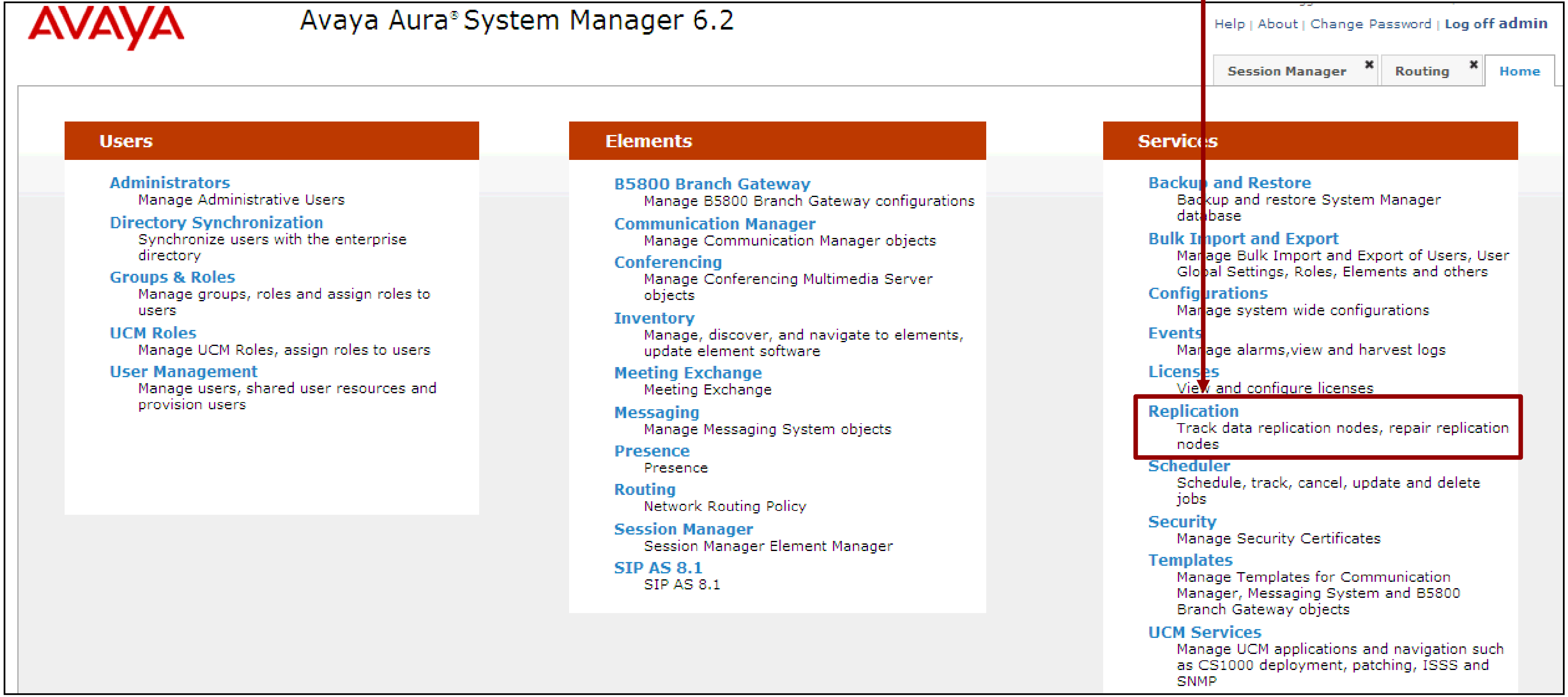
9 Items

☑	Test Description	Test Result	Test Result Time Stamp
☑	Test Call Processing status	Success	Sun Dec 18 01:54:02 GMT+00:00 2011
☑	Test data distribution and redundancy link	Success	Sun Dec 18 01:54:02 GMT+00:00 2011
☑	Test management link functionality	Success	Sun Dec 18 01:54:02 GMT+00:00 2011
☑	Test Postgres database sanity	Success	Sun Dec 18 01:54:02 GMT+00:00 2011
☑	Test sanity of Secure Access Link (SAL) agent	Success	Sun Dec 18 01:54:02 GMT+00:00 2011
☑	Test Security Module status	Success	Sun Dec 18 01:54:03 GMT+00:00 2011
☑	Test Service Director status	Success	Sun Dec 18 01:54:02 GMT+00:00 2011
☑	Test Service Host status	Success	Sun Dec 18 01:54:02 GMT+00:00 2011
☑	Test SIP A/S Management Server status	Success	Sun Dec 18 01:54:02 GMT+00:00 2011

Select : All, None

Data Replication Status

- To check whether System Manager's master database was replicated to your Session Manager, go to the Services column and select **Replication**.



Avaya Aura® System Manager 6.2

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

UCM Roles
Manage UCM Roles, assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway configurations

Communication Manager
Manage Communication Manager objects

Conferencing
Manage Conferencing Multimedia Server objects

Inventory
Manage, discover, and navigate to elements, update element software

Meeting Exchange
Meeting Exchange

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

Scheduler
Schedule, track, cancel, update and delete jobs

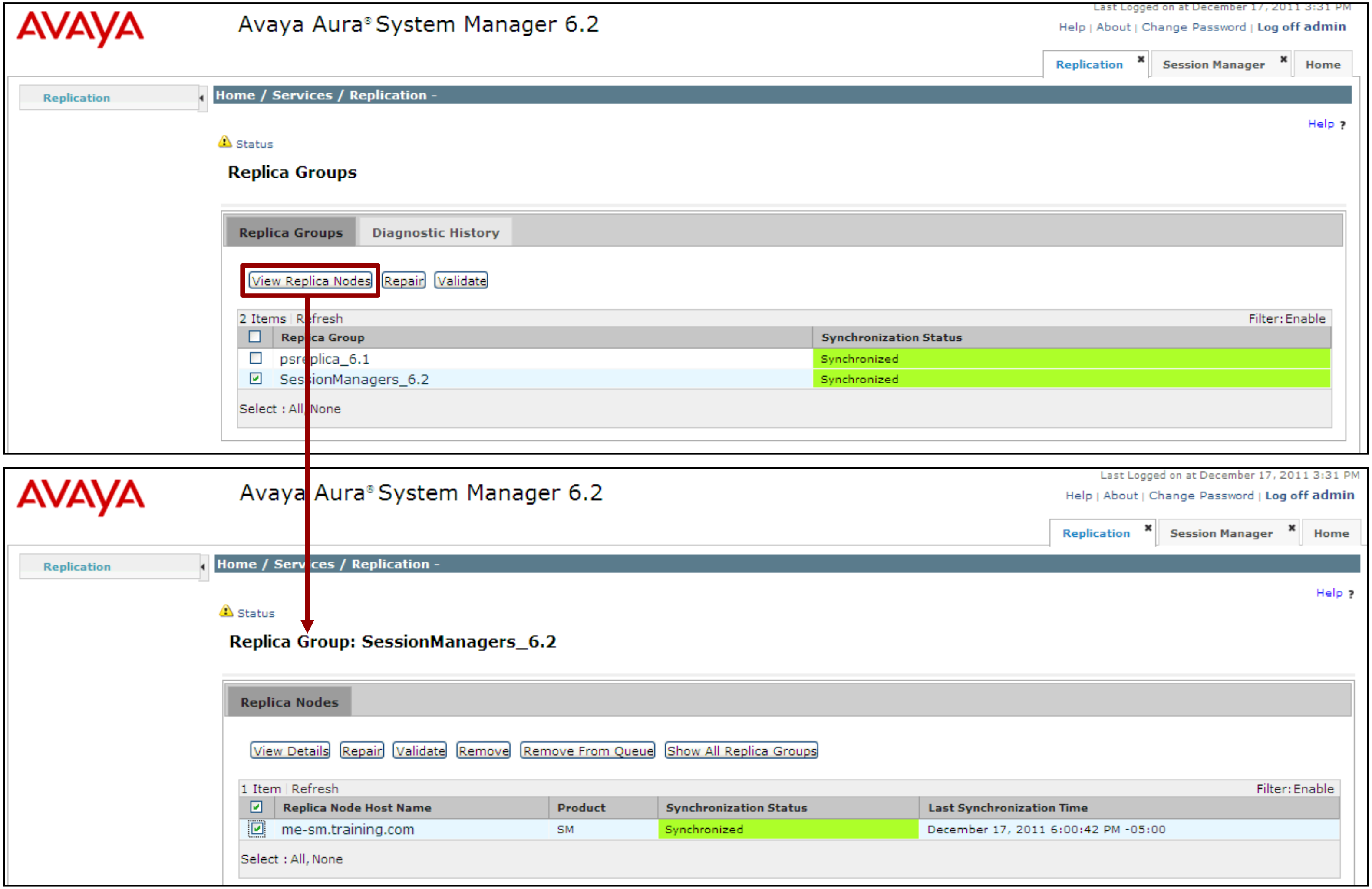
Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway objects

UCM Services
Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

Data Replication Status (continued)

- Validate Synchronization

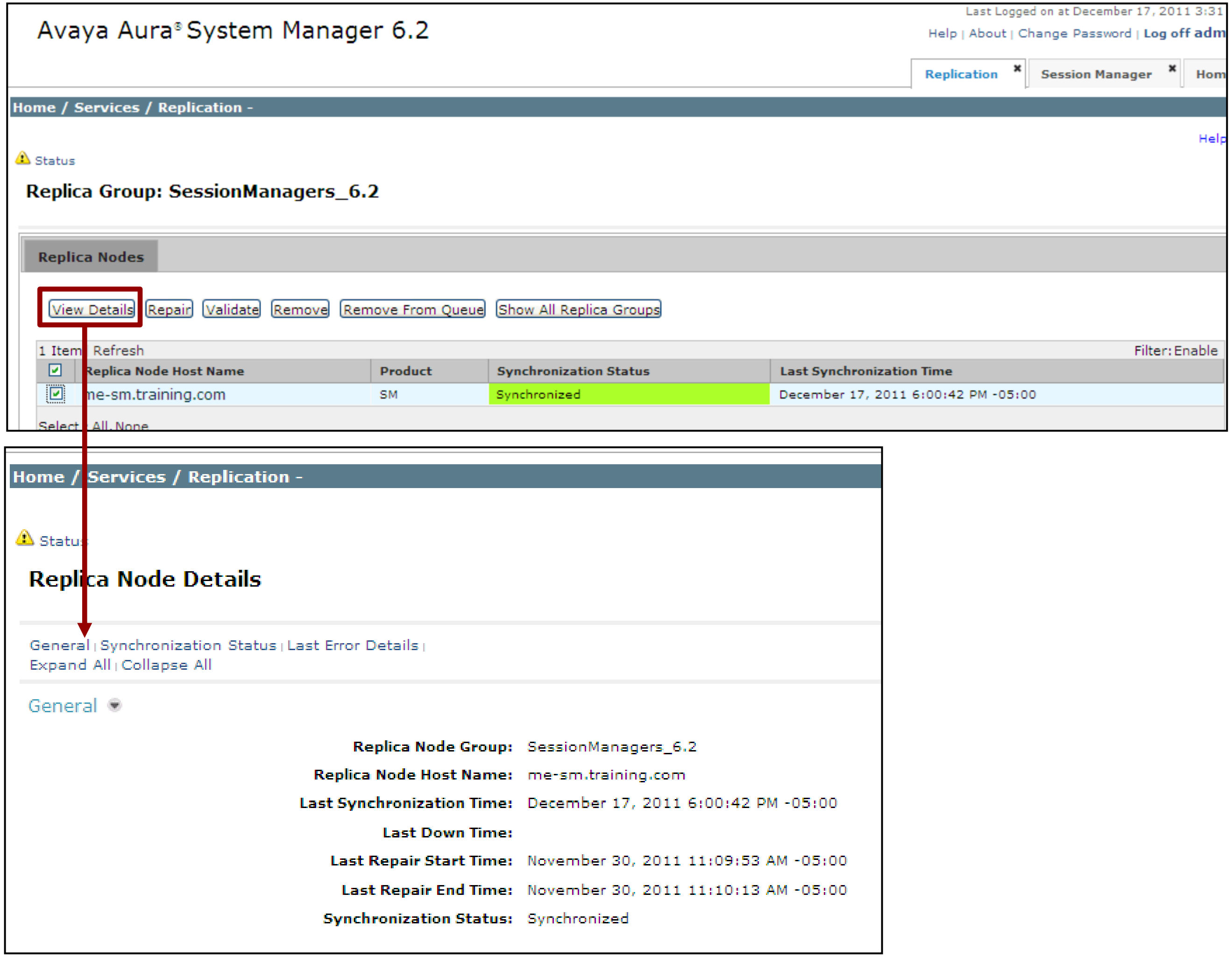


☐	Replica Group	Synchronization Status
☐	psreplica_6.1	Synchronized
☑	SessionManagers_6.2	Synchronized

☑	Replica Node Host Name	Product	Synchronization Status	Last Synchronization Time
☑	me-sm.training.com	SM	Synchronized	December 17, 2011 6:00:42 PM -05:00

Data Replication Status (continued)

- **“Synchronized”** status refers to the Session Manager replica node matching the master node



Avaya Aura® System Manager 6.2

Last Logged on at December 17, 2011 3:31

Help | About | Change Password | Log off adm
Replication ✖ Session Manager ✖ Hom

Home / Services / Replication -

⚠ Status

Replica Group: SessionManagers_6.2

1 Item | Refresh

Filter: Enable

☑	Replica Node Host Name	Product	Synchronization Status	Last Synchronization Time
☑	me-sm.training.com	SM	Synchronized	December 17, 2011 6:00:42 PM -05:00

Select : All, None

Home / Services / Replication -

⚠ Status

Replica Node Details

General | Synchronization Status | Last Error Details |
Expand All | Collapse All

General

Replica Node Group: SessionManagers_6.2

Replica Node Host Name: me-sm.training.com

Last Synchronization Time: December 17, 2011 6:00:42 PM -05:00

Last Down Time:

Last Repair Start Time: November 30, 2011 11:09:53 AM -05:00

Last Repair End Time: November 30, 2011 11:10:13 AM -05:00

Synchronization Status: Synchronized

Exercise: Post Configuration Checks

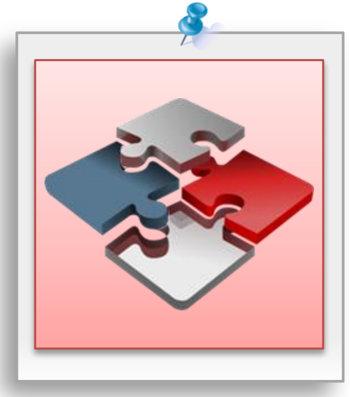
Step	Action
1	Enable the Session Manager to ***Accept New Services***
2	Verify Status of Session Manager
3	Verify Database Replication = *Synchronized*

Lesson Summary

You have completed the following lesson objectives:

Build the following SIP Network components:

- Define the Secure SIP Domain
- Define a Location
- Define Session Manager SIP Entity
- Define Session Manager Instance
- Enable Session Manager to Accept Services
- Complete Post-Configuration Checks



AVAYA | LEARNING

Module 04

Centralized Routing I: SIP Registration and SIP Registry Routing

AVAYA | LEARNING

Lesson 01

SIP Registration and SIP Registry Routing

SIP Registration

- Session Manager checks for a SIP User Profile
- If profile exists, checks registry for registration details (extension/IP address)
- If registered, gets destination location from registry and proxies on
- Else rejects the call, or other call processing if defined

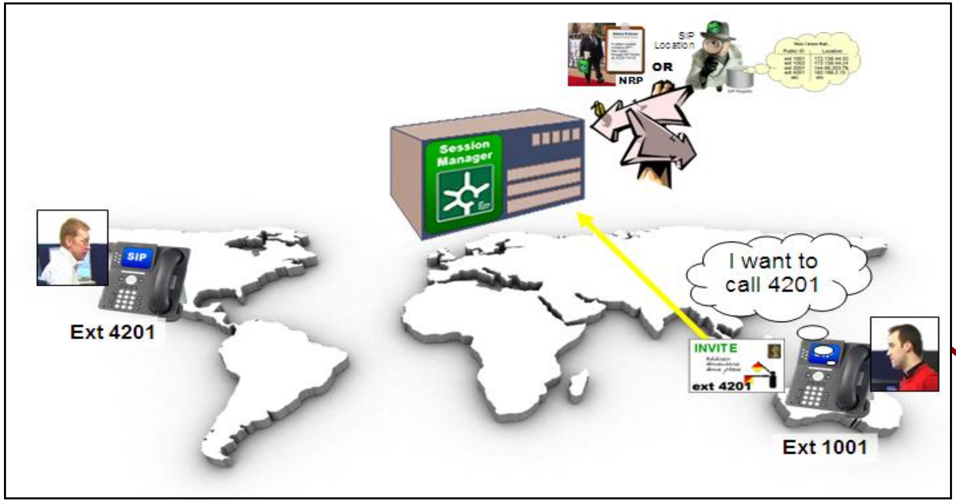
Now I know that…
Public ID
Location
ext 4201
192.168.2.13
Session Manager
REGISTER
192.168.0.210:3002

REGISTRATION

Two bits of info included in a SIP Register request to ASM:
1. SIP URI= ext@avaya.com or +17869886544@avaya.com
2. Location= IP Address

SIP REGISTRY ROUTING

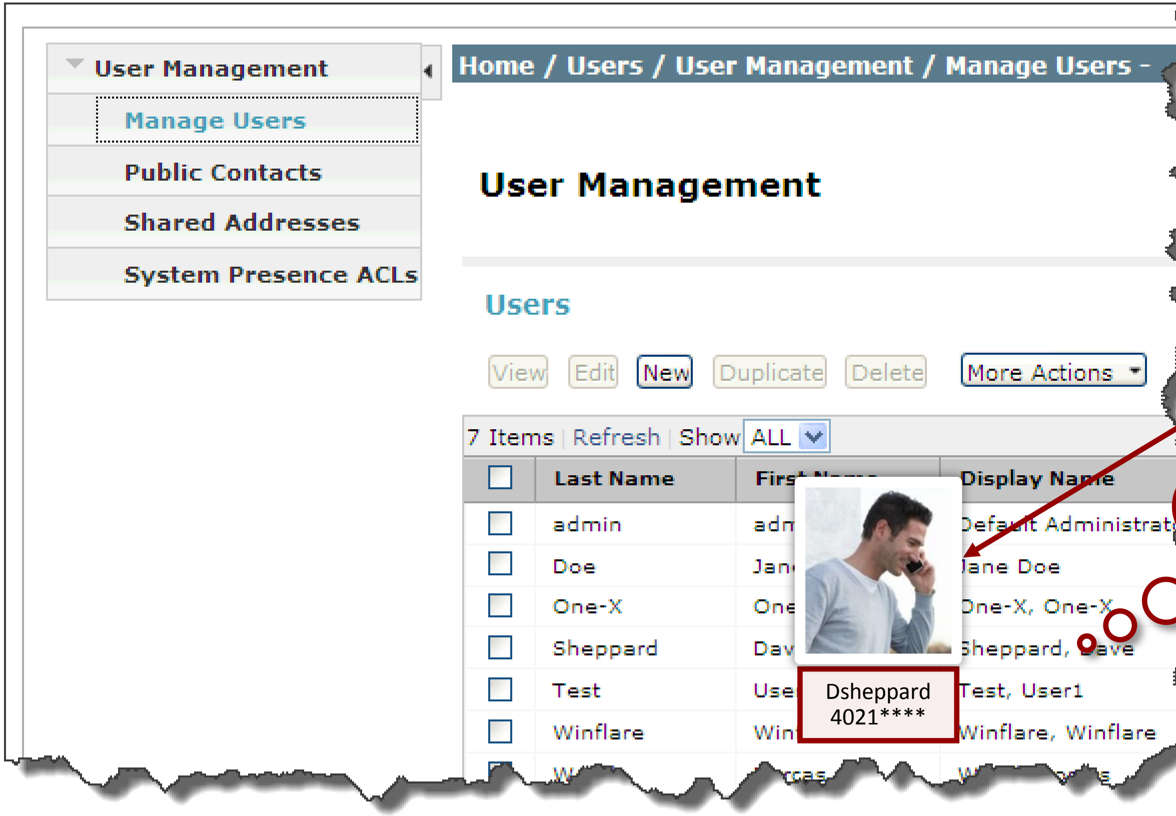
Q. What determines whether ASM will use NRP or SIP Registry Routing?



SIP REGISTRY ROUTING

User Profile

Administrators are responsible for creating SIP User Profiles in System Manager.



- User Management
  - Manage Users
  - Public Contacts
  - Shared Addresses
  - System Presence ACLs

Home / Users / User Management / Manage Users -

User Management

Users

7 Items | Refresh | Show ALL

□	Last Name	First Name	Display Name
□	admin	adm	Default Administrat
□	Doe	Jan	Jane Doe
□	One-X	One	One-X, One-X
□	Sheppard	Dav	Sheppard, Dave
□	Test	Use	Test, User1
□	Winflare	Win	Winflare, Winflare

Dsheppard
4021****

Administrator

https

User Name:	jdoe
Handle (ext):	4201
Password:	****

User Profile

Lesson Summary

You have completed the following lesson objectives:

- Describe Session Manager’s role as a Registrar and in Registry Routing

AVAYA | LEARNING

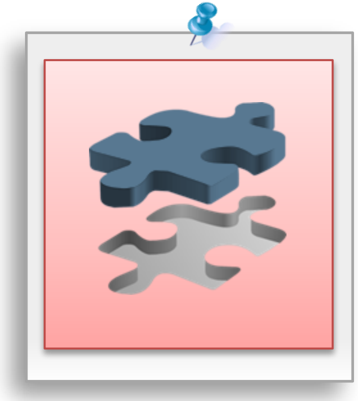
Lesson 02

Setting up the SIP user

Lesson Objective

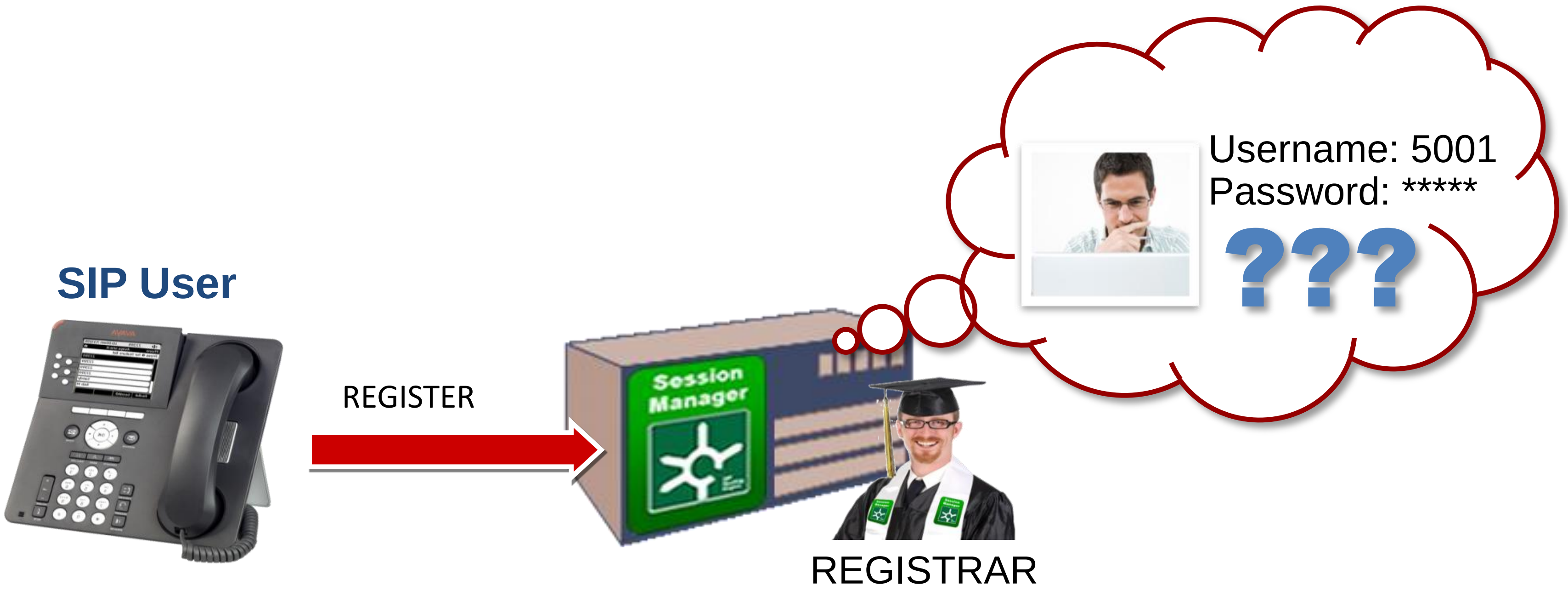
After completing this lesson, you will be able to:

- Create a SIP User



Session Manager User Communication Profile

Create New User for SIP Registration



SIP User

REGISTER

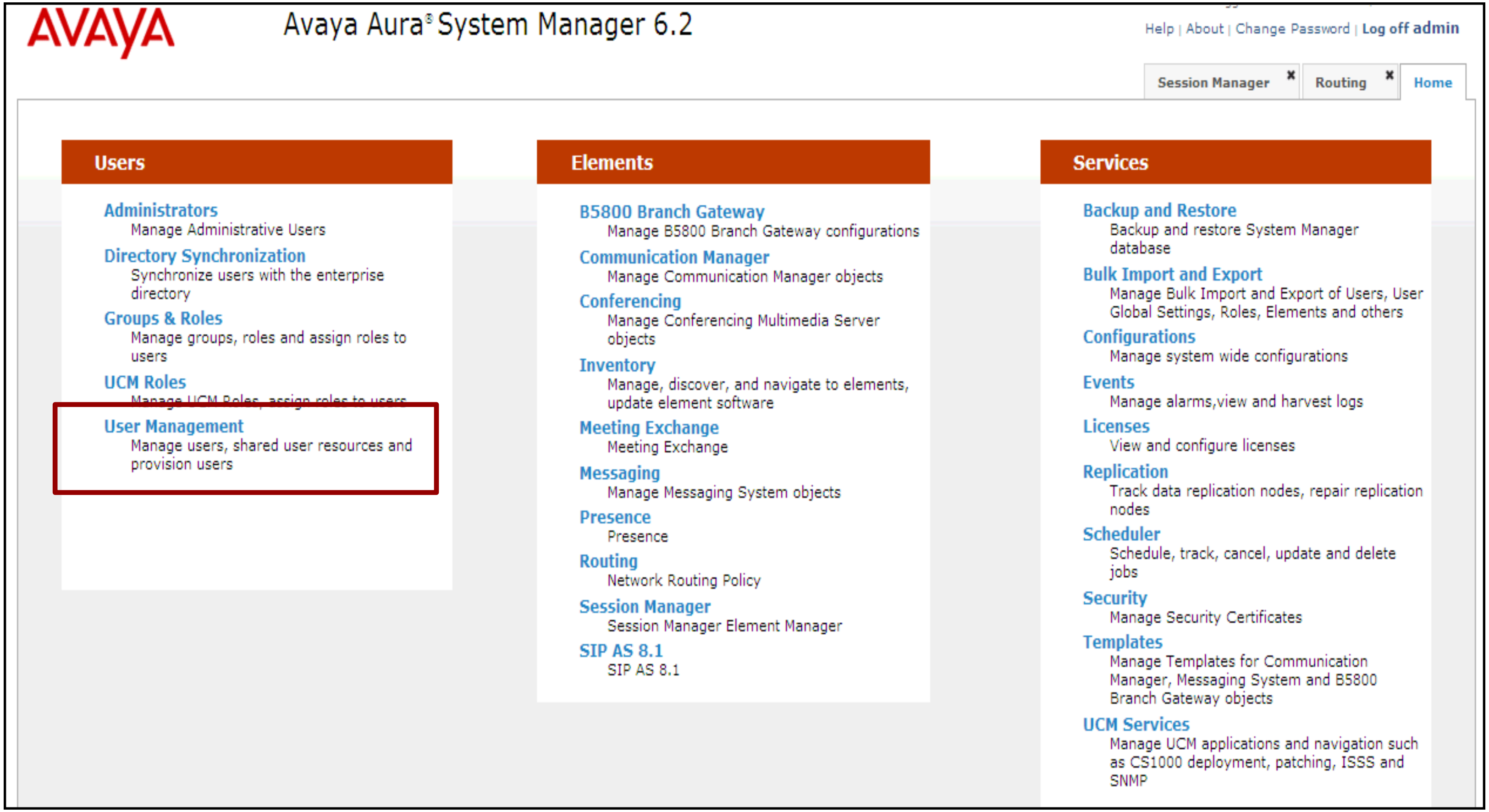
REGISTRAR

Username: 5001
Password: *****

???

Creating User Profiles

- User administration is done through the User Management Menu



AVAYA
Avaya Aura® System Manager 6.2
Help | About | Change Password | Log off admin
Session Manager
Routing
Home

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

UCM Roles
Manage UCM Roles, assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway configurations

Communication Manager
Manage Communication Manager objects

Conferencing
Manage Conferencing Multimedia Server objects

Inventory
Manage, discover, and navigate to elements, update element software

Meeting Exchange
Meeting Exchange

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

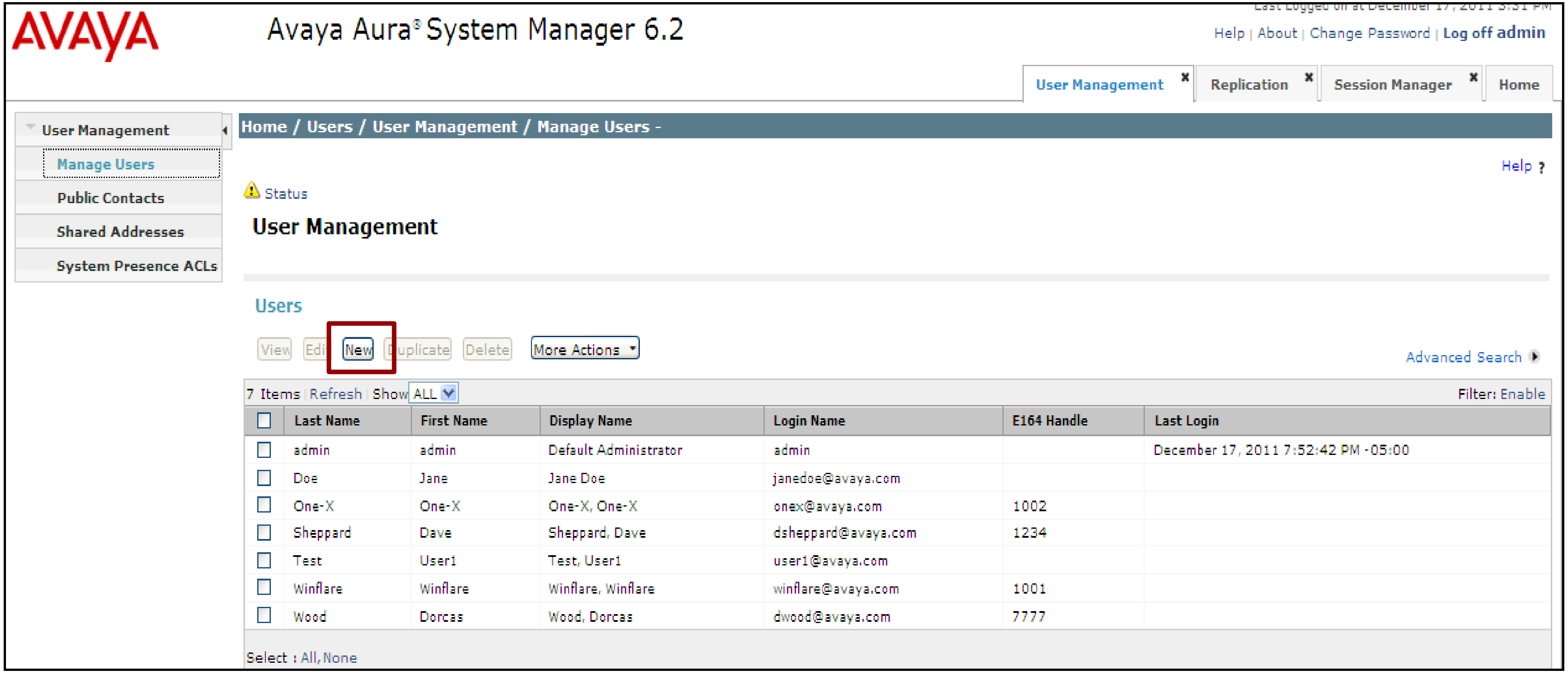
Scheduler
Schedule, track, cancel, update and delete jobs

Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway objects

UCM Services
Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

Creating User Profiles (continued)

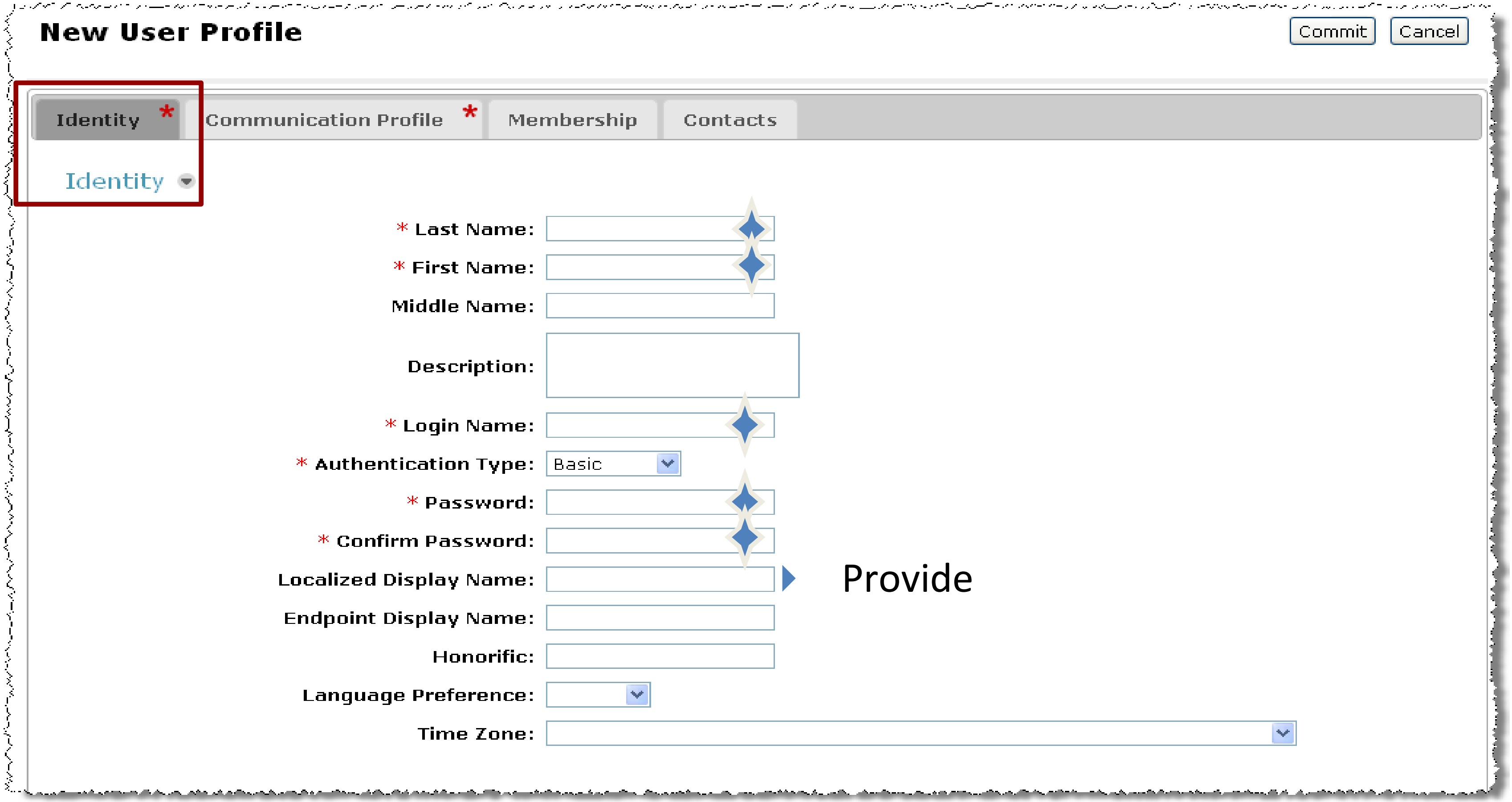


User Management

Users

□	Last Name	First Name	Display Name	Login Name	E164 Handle	Last Login
□	admin	admin	Default Administrator	admin		December 17, 2011 7:52:42 PM -05:00
□	Doe	Jane	Jane Doe	janedoe@avaya.com		
□	One-X	One-X	One-X, One-X	onex@avaya.com	1002	
□	Sheppard	Dave	Sheppard, Dave	dsheppard@avaya.com	1234	
□	Test	User1	Test, User1	user1@avaya.com		
□	Winflare	Winflare	Winflare, Winflare	winflare@avaya.com	1001	
□	Wood	Dorcas	Wood, Dorcas	dwood@avaya.com	7777	

Creating User Profiles (continued)

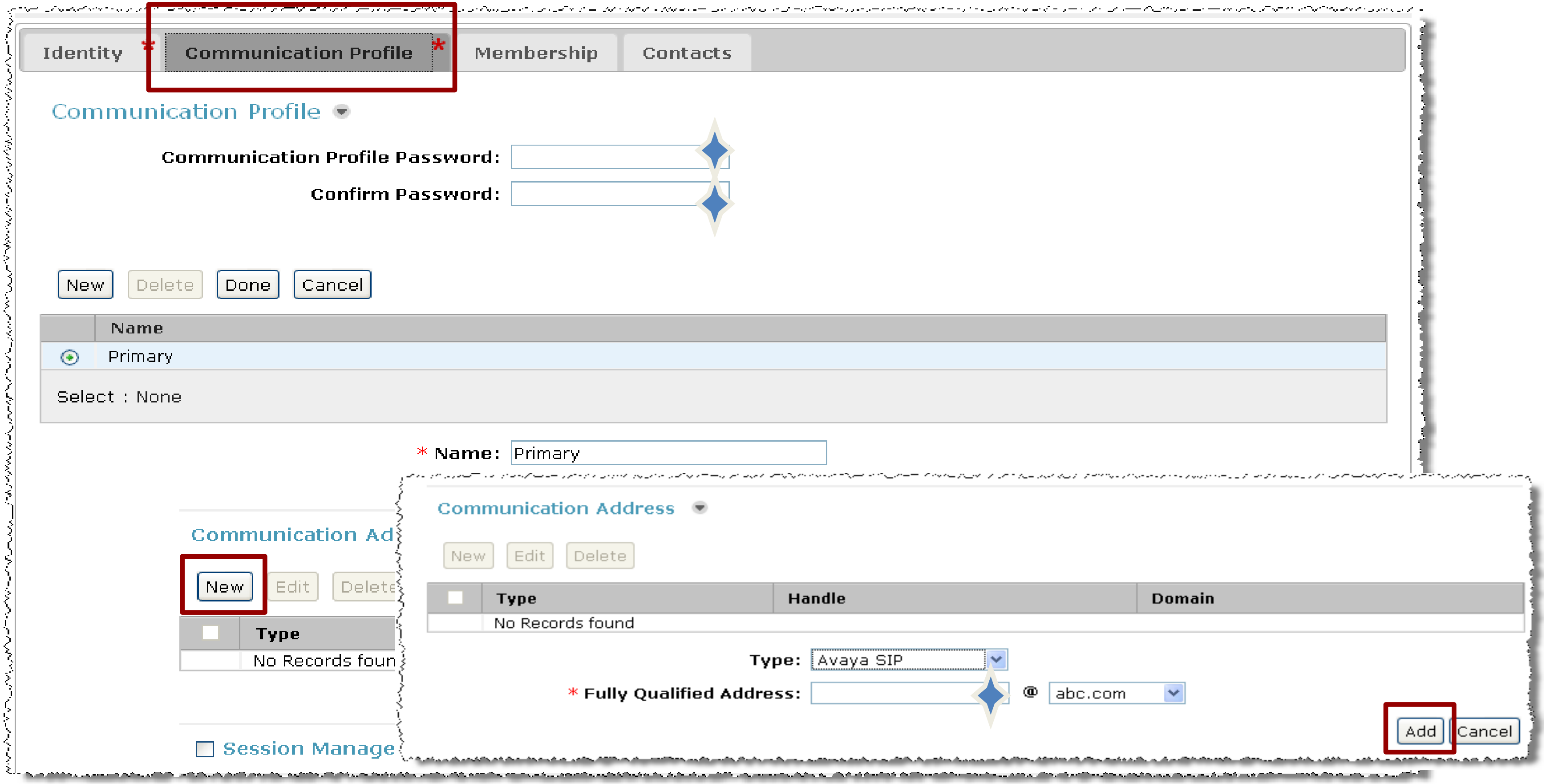


New User Profile

* Last Name:	
* First Name:	
Middle Name:	
Description:	
* Login Name:	
* Authentication Type:	Basic
* Password:	
* Confirm Password:	
Localized Display Name:	
Endpoint Display Name:	
Honorific:	
Language Preference:	
Time Zone:	

Provide

User Profile – The Communication Profile



Identity * | Communication Profile * | Membership | Contacts

Communication Profile

Communication Profile Password:

Confirm Password:

New | Delete | Done | Cancel

	Name
●	Primary

Select : None

* Name: Primary

Communication Ad

New | Edit | Delete

□	Type
	No Records foun

□ Session Manage

Communication Address

New | Edit | Delete

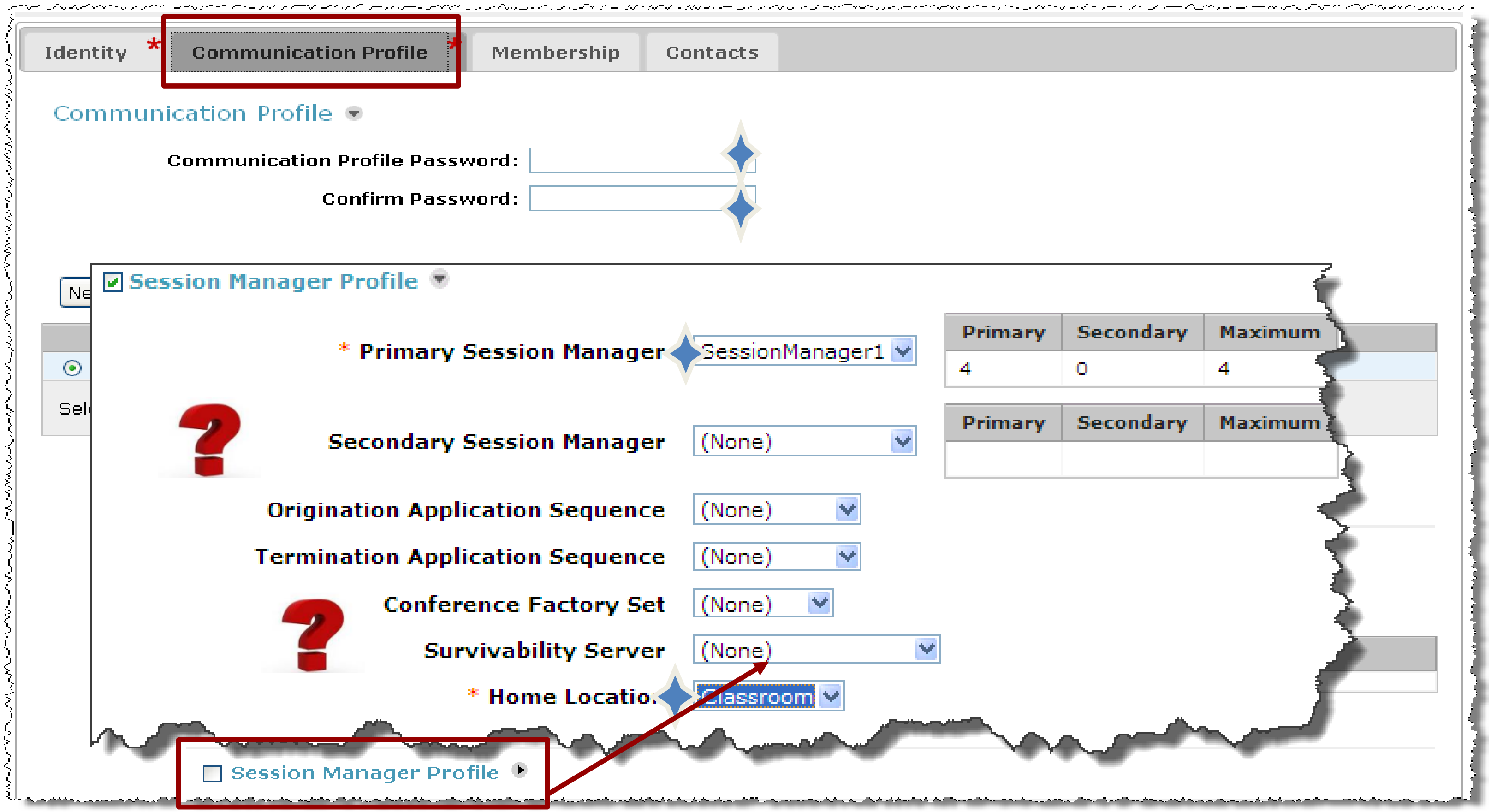
□	Type	Handle	Domain
	No Records found		

Type: Avaya SIP

* Fully Qualified Address: @ abc.com

Add | Cancel

Creating Communication Profiles



Communication Profile

Communication Profile Password:

Confirm Password:

☑ Session Manager Profile

* Primary Session Manager: SessionManager1

Primary	Secondary	Maximum
4	0	4

Secondary Session Manager: (None)

Primary	Secondary	Maximum

Origination Application Sequence: (None)

Termination Application Sequence: (None)

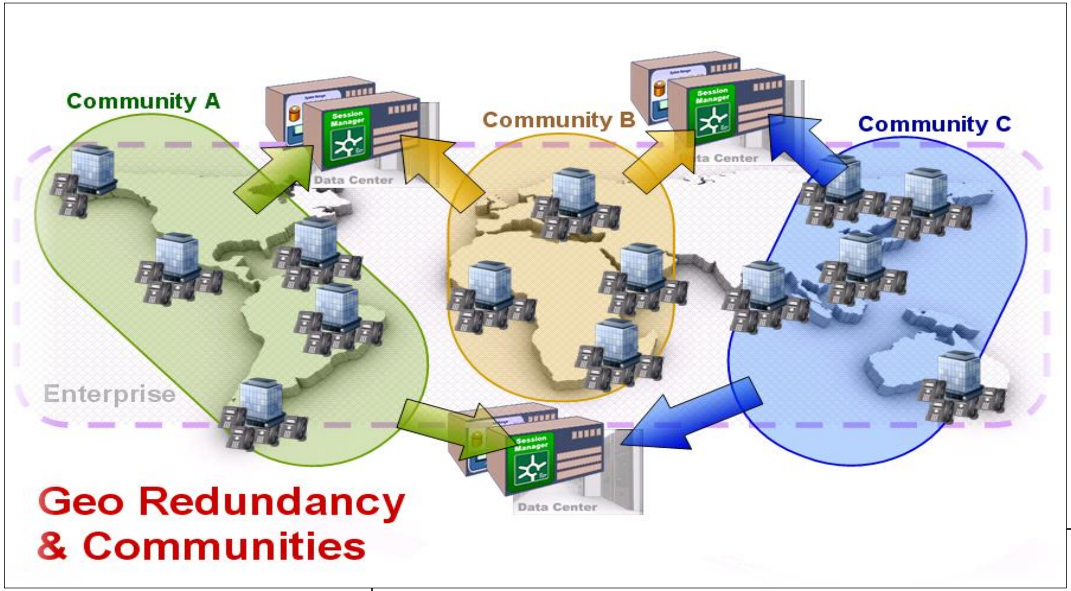
Conference Factory Set: (None)

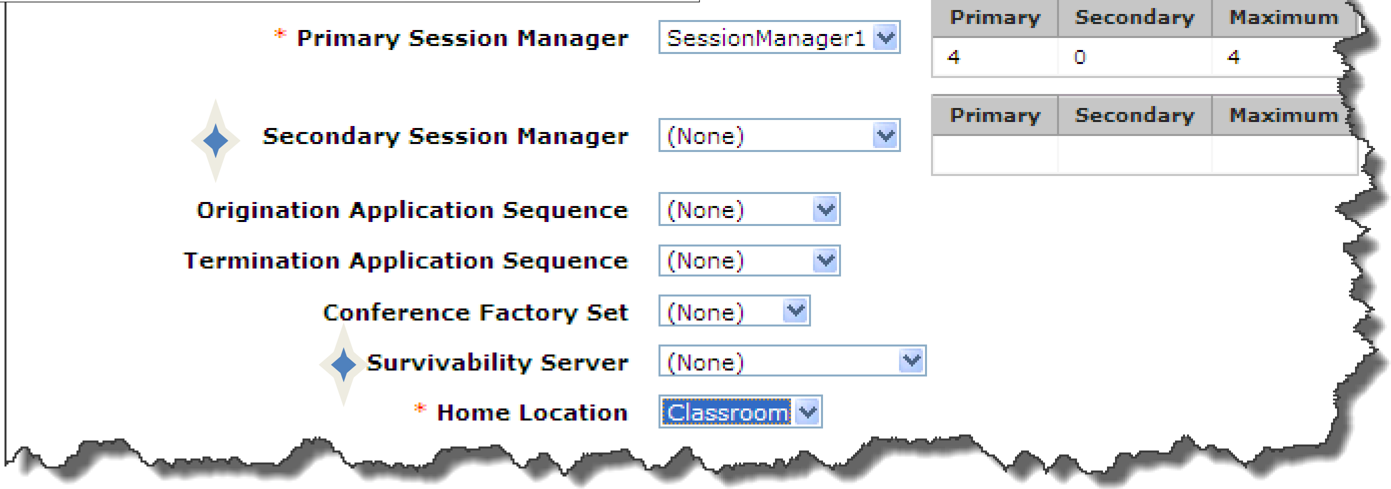
Survivability Server: (None)

* Home Locatio: Classroom

□ Session Manager Profile

SIP Users and Redundancy



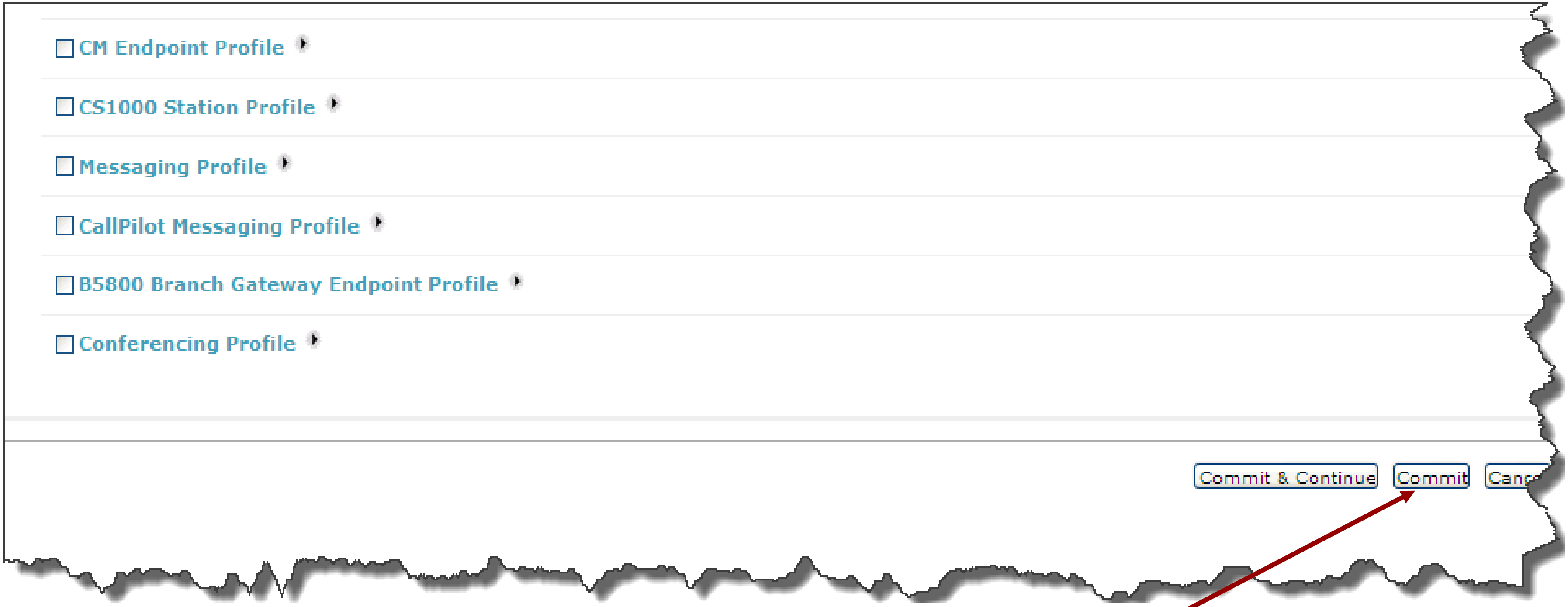


* Primary Session Manager	SessionManager1
Secondary Session Manager	(None)
Origination Application Sequence	(None)
Termination Application Sequence	(None)
Conference Factory Set	(None)
Survivability Server	(None)
* Home Location	Classroom

Primary	Secondary	Maximum
4	0	4

Primary	Secondary	Maximum

Creating User Profiles



- □ CM Endpoint Profile
- □ CS1000 Station Profile
- □ Messaging Profile
- □ CallPilot Messaging Profile
- □ B5800 Branch Gateway Endpoint Profile
- □ Conferencing Profile

Once happy, select ‘**Commit**’

Exercise: Create SIP Communication Profile x9x1

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>At System Manager console select <em>User Management</em> Menu</td></tr>
<tr><td>2</td><td>Select <strong>New</strong></td></tr>
<tr><td>3</td><td><strong><u>On the Identity Tab:</u></strong><ul><li>Add First/Last Name: <em>Your name</em></li><li>Login Name: email address format i.e. <strong>yourname@avaya.com</strong></li><li>Password (alpha-numeric format, 7 digit minimum): <strong>Passw0rd!</strong></li></ul></td></tr>
<tr><td>4</td><td><strong><u>On the Communication Profile Tab:</u></strong>
Password: Enter <strong>123456</strong><ul><li>Go down to Communication Address</li><li>Select <strong><em>New</em></strong></li><li>Type: <strong><em>Avaya SIP</em></strong></li><li>Fully qualified address: <em>1911</em><strong>@training.com</strong></li></ul>
<table>
<tr><th>Student</th><th>Pod 1</th><th>Pod 2</th><th>Pod 3</th><th>Pod 4</th><th>Pod 5</th><th>Pod 6</th></tr>
<tr><td><strong>Student a</strong></td><td><strong>1911</strong></td><td><strong>2911</strong></td><td><strong>3911</strong></td><td><strong>4911</strong></td><td><strong>5911</strong></td><td><strong>6911</strong></td></tr>
<tr><td><strong>Student b</strong></td><td><strong>1921</strong></td><td><strong>2921</strong></td><td><strong>3921</strong></td><td><strong>4921</strong></td><td><strong>5921</strong></td><td><strong>6921</strong></td></tr>
</table>
<strong>Select Add</strong></td></tr>
<tr><td>5</td><td><strong><u>Session Manager Profile</u></strong>
Assign the user to your assigned Session Manager
Location: <strong>Denver</strong></td></tr>
<tr><td>6</td><td><strong><em>Commit</em></strong></td></tr>
</table>

Exercise: Create New User Communication Profile x9x2

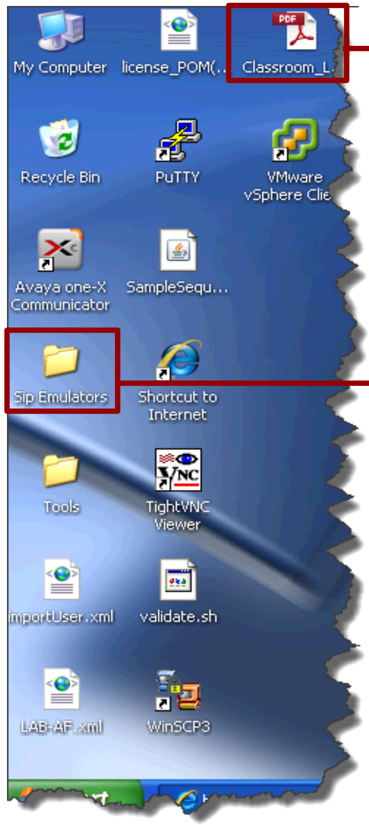
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>At System Manager console select User Management Menu</td></tr>
<tr><td>2</td><td>Select <b>New</b></td></tr>
<tr><td>3</td><td><b><u>On the Identity Tab:</u></b>
● Add First/Last Name: <i>Your name</i>
● Login Name: email address format i.e. <b>yourname@avaya.com</b>
● Password: alpha-numeric format. 7 digit minimum i.e. <b>Passw0rd!</b></td></tr>
<tr><td>4</td><td><b><u>On the Communication Profile Tab:</u></b>
Password: Enter <b>123456</b>
● Go down to Communication Address
● Select <b><i>New</i></b>
● Type: <b><i>Avaya SIP</i></b>
● Fully qualified address: 1912@<b>training.com</b>
<table>
<tr><th>Student</th><th>Pod 1</th><th>Pod 2</th><th>Pod 3</th><th>Pod 4</th><th>Pod 5</th><th>Pod 6</th></tr>
<tr><td><b>Student a</b></td><td><b>1912</b></td><td><b>2912</b></td><td><b>3912</b></td><td><b>4912</b></td><td><b>5912</b></td><td><b>6912</b></td></tr>
<tr><td><b>Student b</b></td><td><b>1922</b></td><td><b>2922</b></td><td><b>3922</b></td><td><b>4922</b></td><td><b>5922</b></td><td><b>6922</b></td></tr>
</table>
<b>Select Add</b></td></tr>
<tr><td>5</td><td><b><u>Session Manager Profile</u></b>
Assign the user to your assigned Session Manager
Location: <b>Denver</b></td></tr>
<tr><td>6</td><td><b>Commit</b></td></tr>
</table>

Register System Manager SIP User

Register System Manager SIP User

The next exercise will show you how to configure the One-X SIP Phone Emulator to Register to Session Manager.

Before you can register your new user, you must configure the SIP Phone to register to Session Manager so it can route it’s SIP sessions.

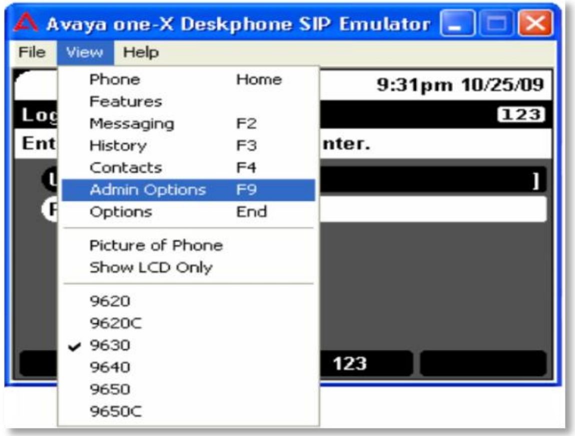


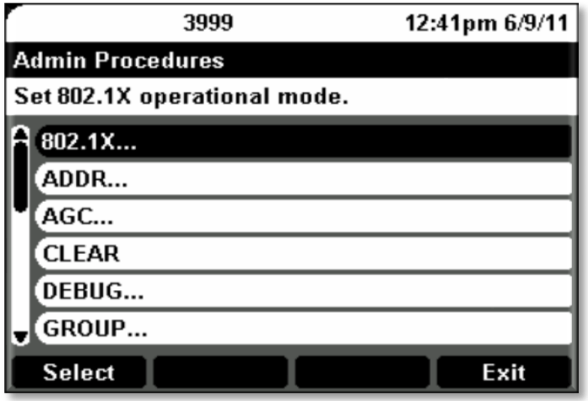
The information needed to configure your SIP phone is located in the Classroom Layout PDF.

Launch the SIP Phone found in the **SIP Emulators folder** on your desktop.

Exercise: Configure SIP Phones

- Open the **SIP Emulators Folder** on the Desktop

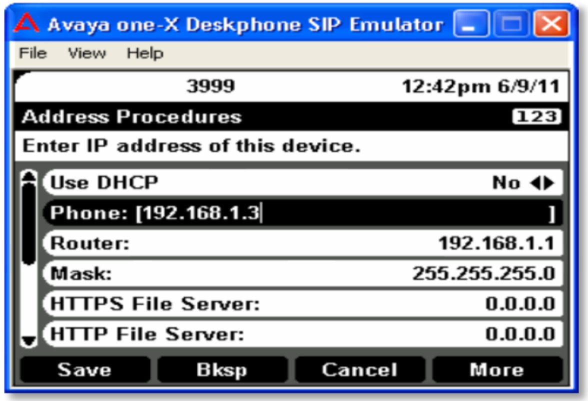




3999 12:41pm 6/9/11

Admin Procedures

Set 802.1X operational mode.



3999 12:42pm 6/9/11

Address Procedures 123

Enter IP address of this device.

Use DHCP No

Phone: [192.168.1.3]

Router: 192.168.1.1

Mask: 255.255.255.0

HTTPS File Server: 0.0.0.0

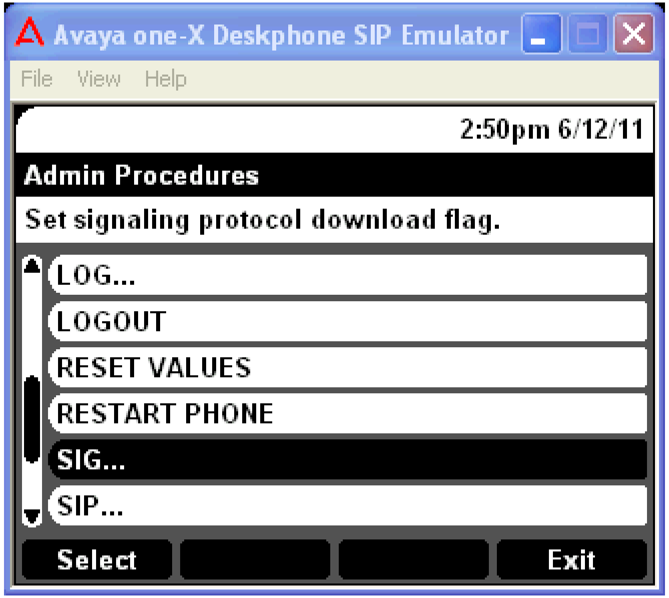
HTTP File Server: 0.0.0.0

1. Navigate to
   View >>Admin Options

2. Select ***ADDR*** Menu
   Student a 172.16.x.11
   Student b 172.16.x.12

3. Router:**172.16.255.254**
   Mask: **255.255.0.0**
   Save

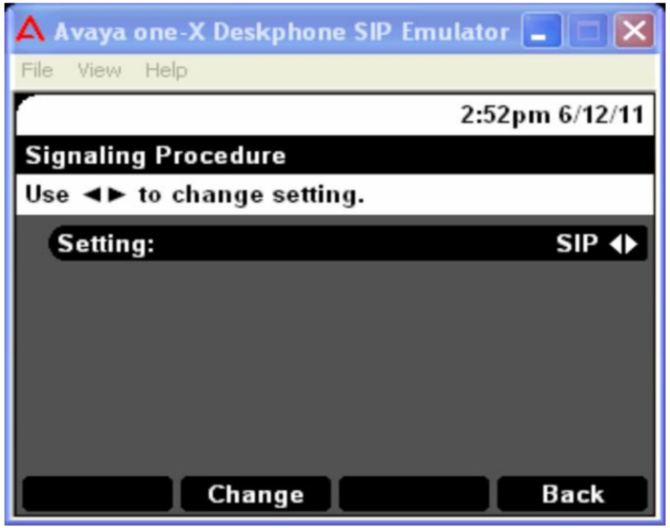
Exercise: Configure SIP Emulator



2:50pm 6/12/11

Admin Procedures

Set signaling protocol download flag.



2:52pm 6/12/11

Signaling Procedure

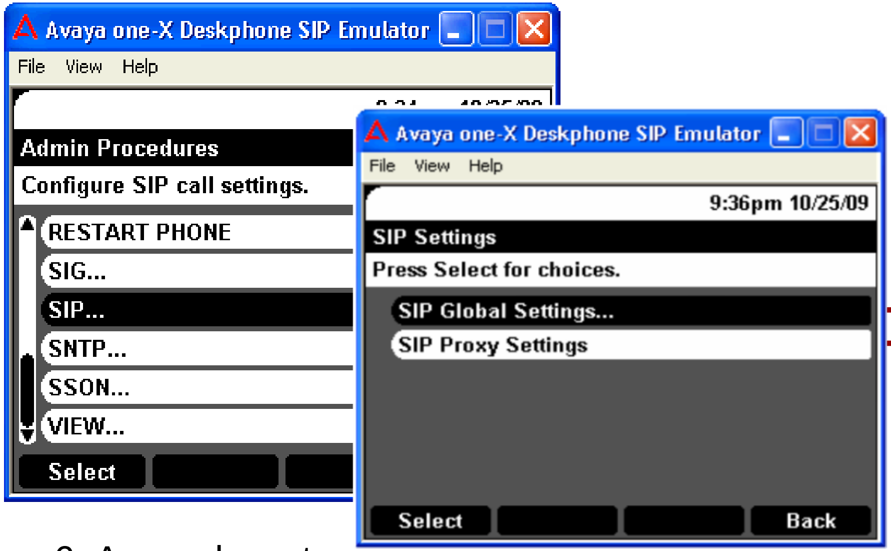
Use ◄► to change setting.

Setting: SIP ◄►

4. Select ***SIG*** Menu

5. Select the **SIP** Protocol: hit right arrow until SIP is selected and Save

Exercise: Configure SIP Emulator (continued)



Avaya one-X Deskphone SIP Emulator

Admin Procedures

Configure SIP call settings.

- RESTART PHONE
- SIG...
- SIP...
- SNTP...
- SSON...
- VIEW...

Avaya one-X Deskphone SIP Emulator

9:36pm 10/25/09

SIP Settings

Press Select for choices.

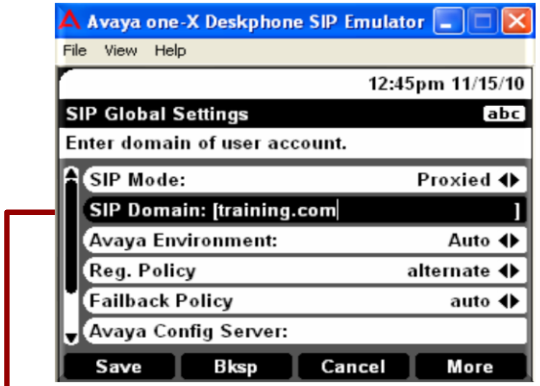
- SIP Global Settings...
- SIP Proxy Settings

6. Arrow down to SIP Menu

7. Configure **SIP Global Settings**:

SIP Mode: **Proxied**

Domain: **training.com**



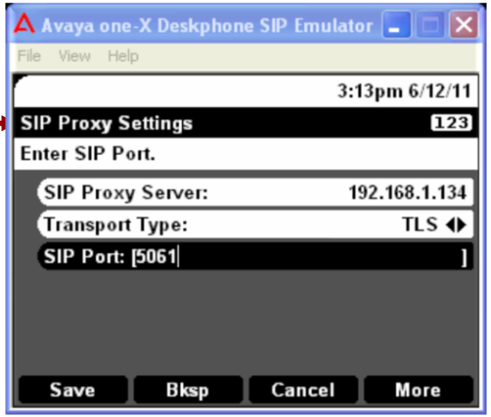
Avaya one-X Deskphone SIP Emulator

12:45pm 11/15/10

SIP Global Settings abc

Enter domain of user account.

SIP Mode:	Proxied
SIP Domain: [training.com	]
Avaya Environment:	Auto
Reg. Policy	alternate
Failback Policy	auto
Avaya Config Server:	



Avaya one-X Deskphone SIP Emulator

3:13pm 6/12/11

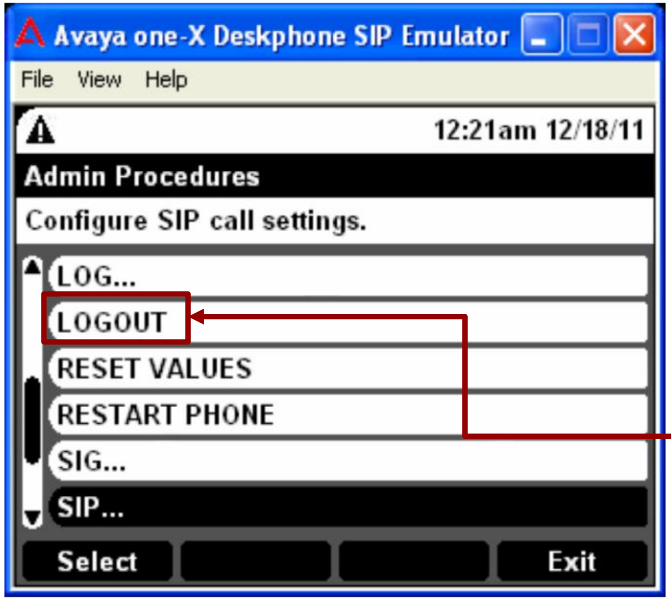
SIP Proxy Settings 123

Enter SIP Port.

SIP Proxy Server:	192.168.1.134
Transport Type:	TLS
SIP Port: [5061	]

8. Arrow down to SIP Proxy Settings:
   SIP Proxy Server:
   Student a: 172.16.x.105
   Student b: 172.16.x.115
   Transport Type: **TLS**
   SIP Port: **5061**

Exercise: Configure SIP Emulator (continued)



Select **Logout** instead

<span style="color:red">Do Not Select *EXIT*</span>

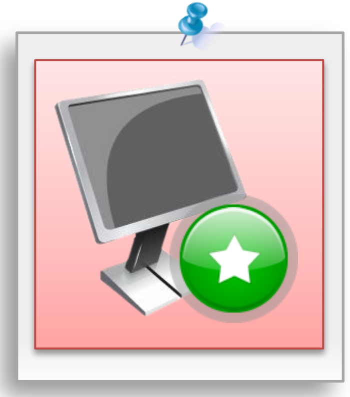
Instead, arrow UP to the **Logout** setting.

(If you EXIT the application will close and not retain your settings.)

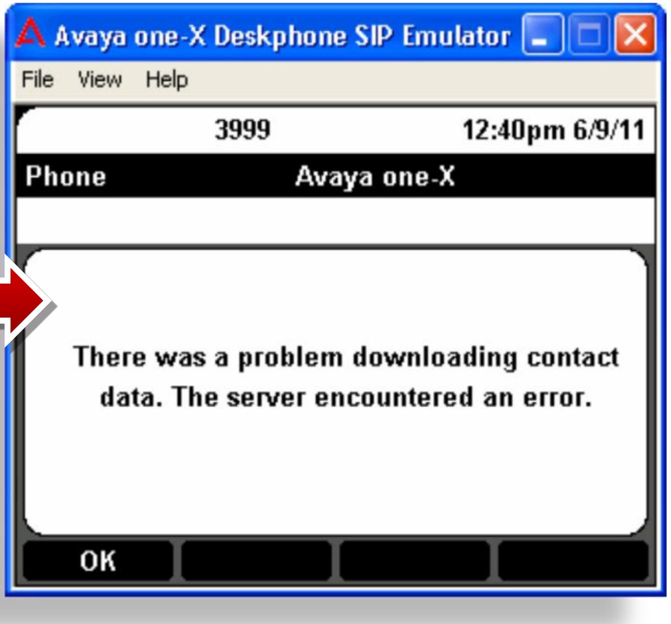
Exercise: Register x9x1 SIP Phone

Step	Action
1	Open the SIP Emulator Folder on the Desktop
2	Double Click **SIP Phone Emulator #1**
3	Log into SIP Phone using extension and password: **123456**

Student	Pod 1	Pod 2	Pod 3	Pod 4	Pod 5	Pod 6
Student a	1911	2911	3911	4911	5911	6911
Student b	1921	2921	3921	4921	5921	6921



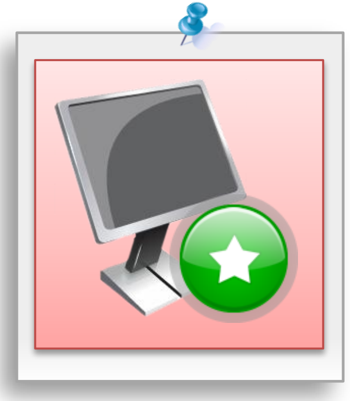
Disregard PPM download error for now and Enter OK.



There was a problem downloading contact data. The server encountered an error.

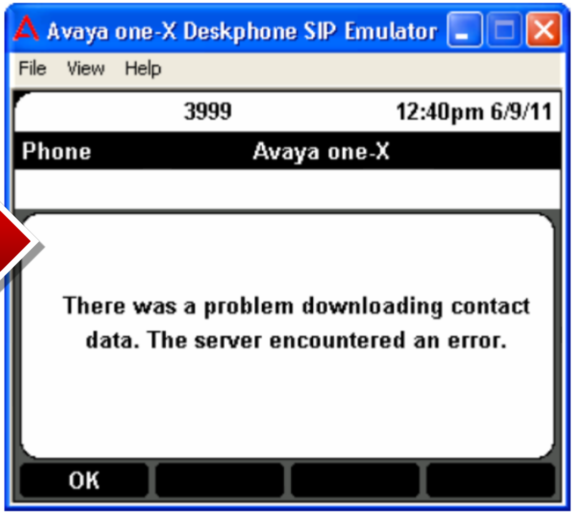
Exercise: Register x9x2 SIP Phone

Step	Action
1	Open the SIP Emulator Folder on the Desktop
2	Double Click **SIP Phone Emulator 2**
3	Log into SIP Phone using extension and password 123456



Student	Pod 1	Pod 2	Pod 3	Pod 4	Pod 5	Pod 6
Student a	1912	2912	3912	4912	5912	6912
Student b	1922	2922	3922	4922	5922	6922

Disregard PPM download error for now and Enter OK.

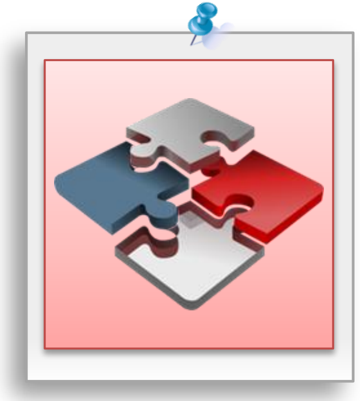


There was a problem downloading contact data. The server encountered an error.

Lesson Summary

You have completed the following lesson objectives:

- Create a SIP User



Lesson 3

SIP Tracing

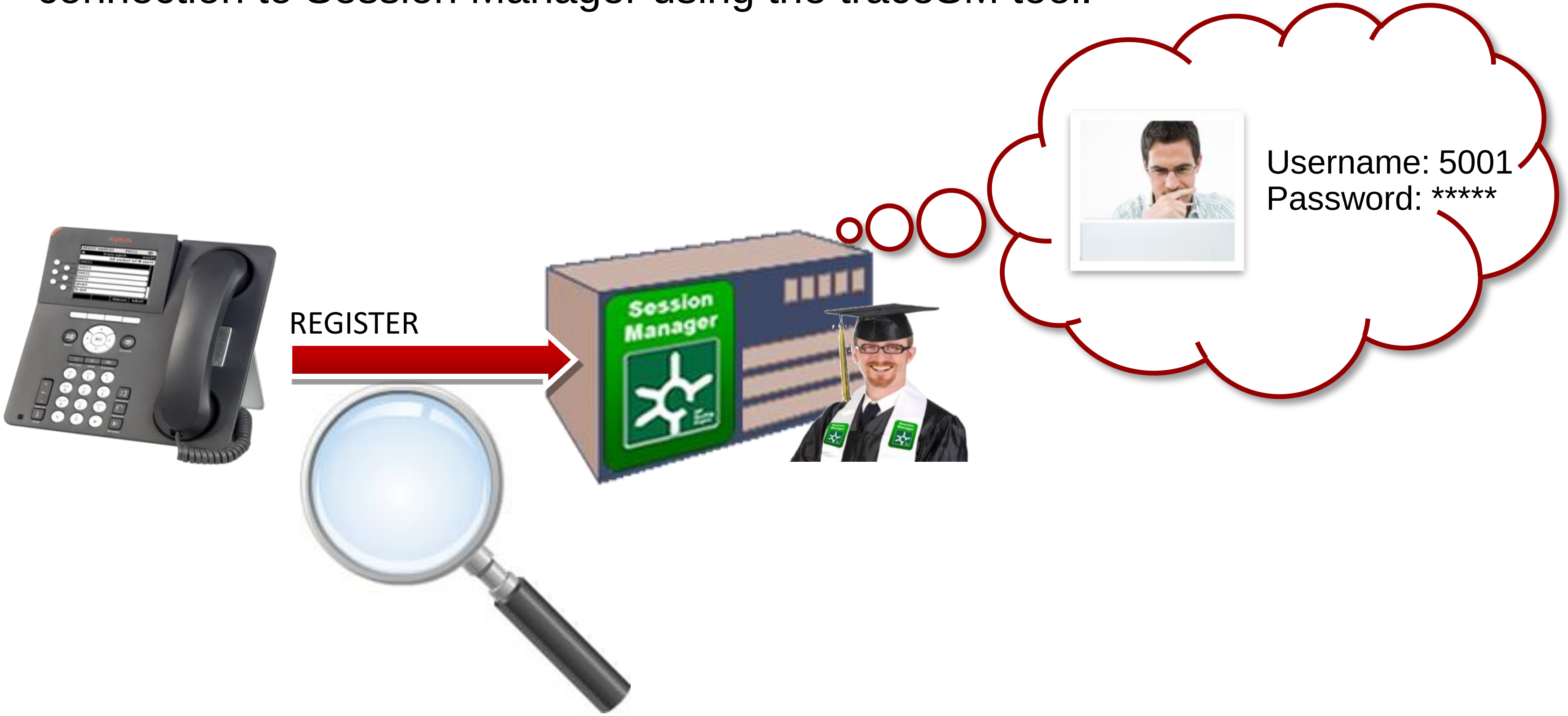
Lesson Objective

After completing this lesson, you will be able to:

- Use SIP tracing tools to view the SIP call flow

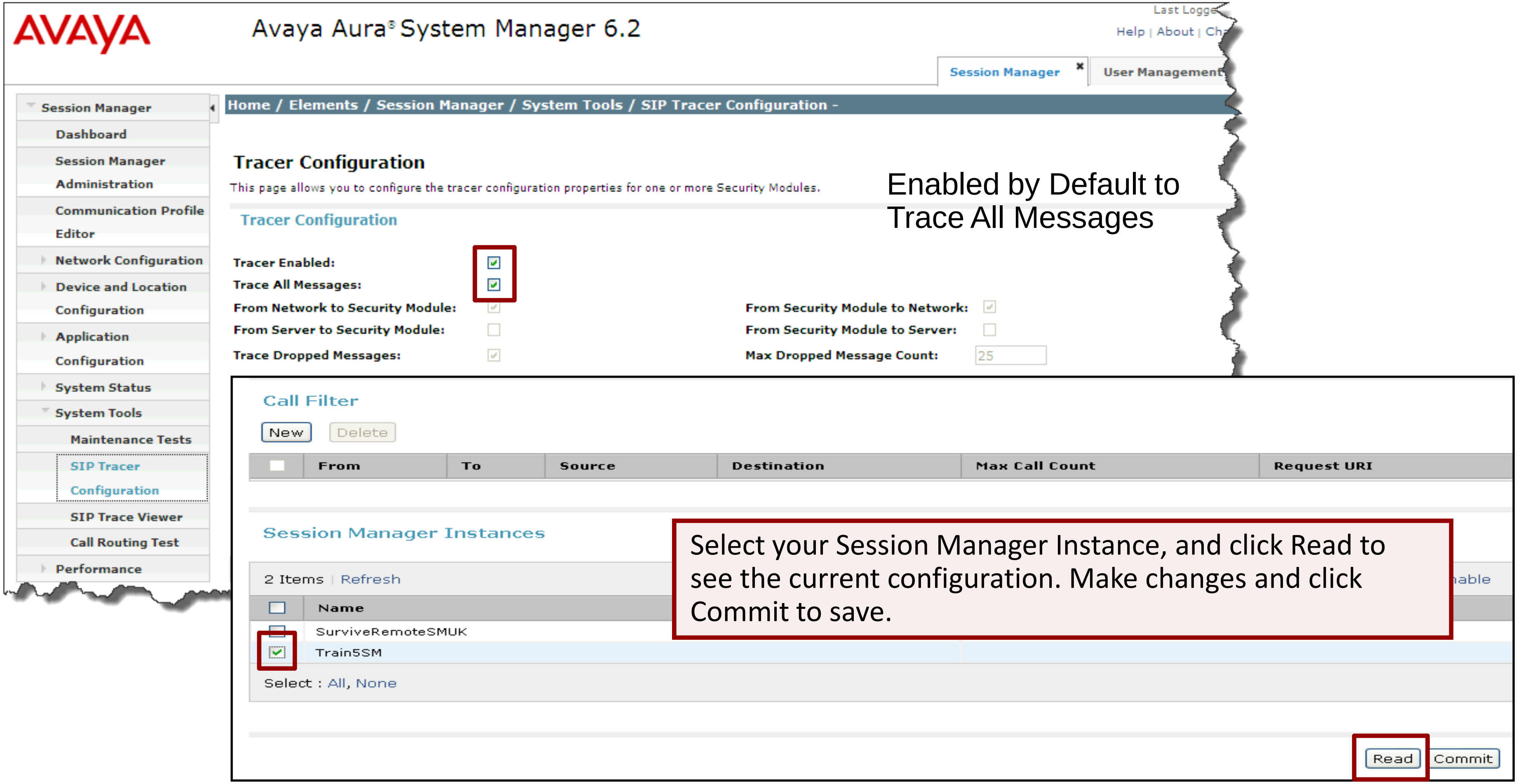
Analyzing the Registration

- There are a couple of ways we can trace a SIP call:
- We can use System Manager Trace Viewer tool or we can establish an SSH connection to Session Manager using the traceSM tool.



SIP Tracer Configuration

- Let’s first configure the Trace Viewer for tracing.
- Go to Session Manager >> SIP Tracer Configuration



Home / Elements / Session Manager / System Tools / SIP Tracer Configuration -

Tracer Configuration

This page allows you to configure the tracer configuration properties for one or more Security Modules.

Tracer Configuration

Tracer Enabled:	☑		
Trace All Messages:	☑		
From Network to Security Module:	☑	From Security Module to Network:	☑
From Server to Security Module:	□	From Security Module to Server:	□
Trace Dropped Messages:	☑	Max Dropped Message Count:	25

Enabled by Default to Trace All Messages

Call Filter

New Delete

□	From	To	Source	Destination	Max Call Count	Request URI

Session Manager Instances

2 Items | Refresh able

□	Name
□	SurviveRemoteSMUK
☑	Train5SM

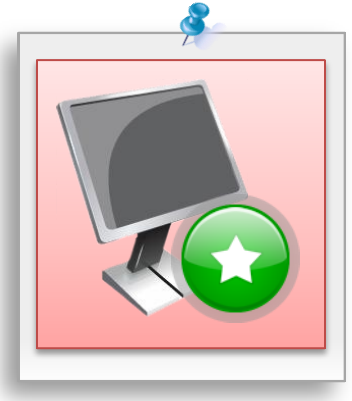
Select : All, None

Read Commit

Select your Session Manager Instance, and click Read to see the current configuration. Make changes and click Commit to save.

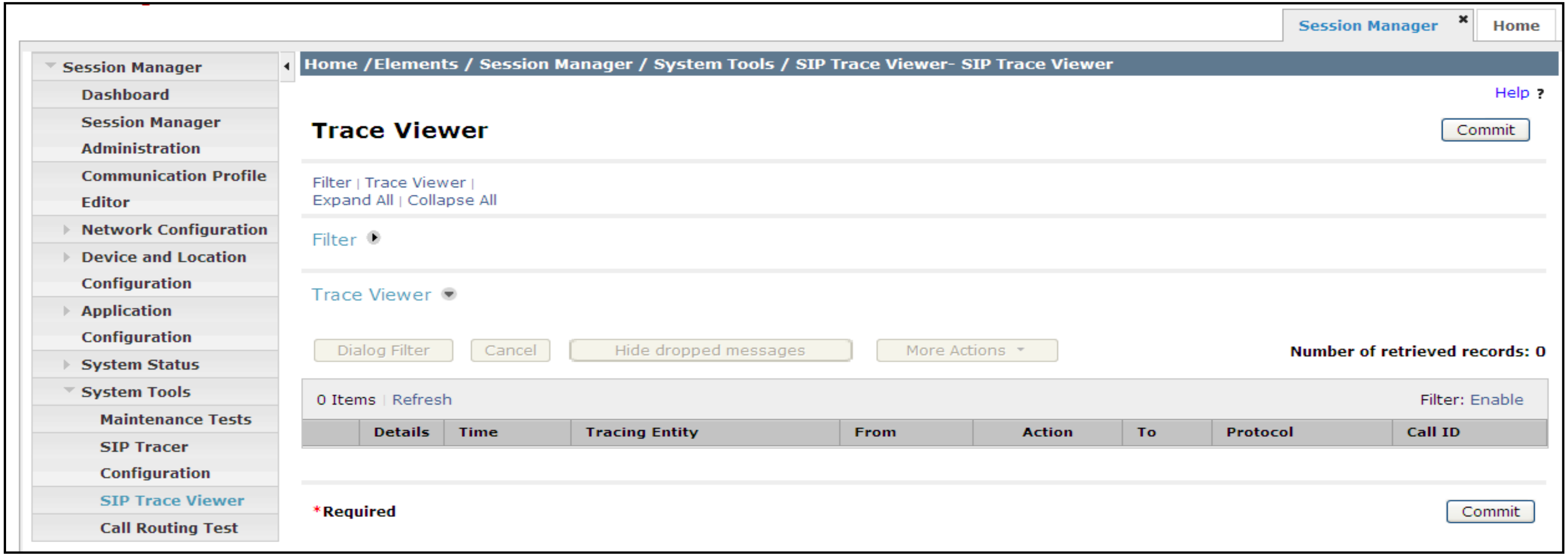
Exercise: Configure SIP Trace Viewer

Step	Action
1	Navigate from the System Manager Home Page to Session Manager Elements Menu >> System Tools >> SIP Tracer Configuration
2	At the bottom, select “YourSessionManager”
3	Click the ***Read*** Button
4	Deselect ***Tracer Enables***
5	Select ***Tracer Enables*** again
6	Select ***Commit***



Viewing the SIP Trace

- Once configured, you can navigate to SIP Trace Viewer, enter a filter and view the results



Session Manager ✖ | Home

- Session Manager
  - Dashboard
  - Session Manager Administration
  - Communication Profile Editor
  - Network Configuration
  - Device and Location Configuration
  - Application Configuration
  - System Status
  - System Tools
    - Maintenance Tests
    - SIP Tracer Configuration
    - SIP Trace Viewer
    - Call Routing Test

Home /Elements / Session Manager / System Tools / SIP Trace Viewer- SIP Trace Viewer

Help ?

Trace Viewer

Commit

Filter | Trace Viewer |
Expand All | Collapse All

Filter

Trace Viewer

Dialog Filter | Cancel | Hide dropped messages | More Actions

Number of retrieved records: 0

0 Items | Refresh

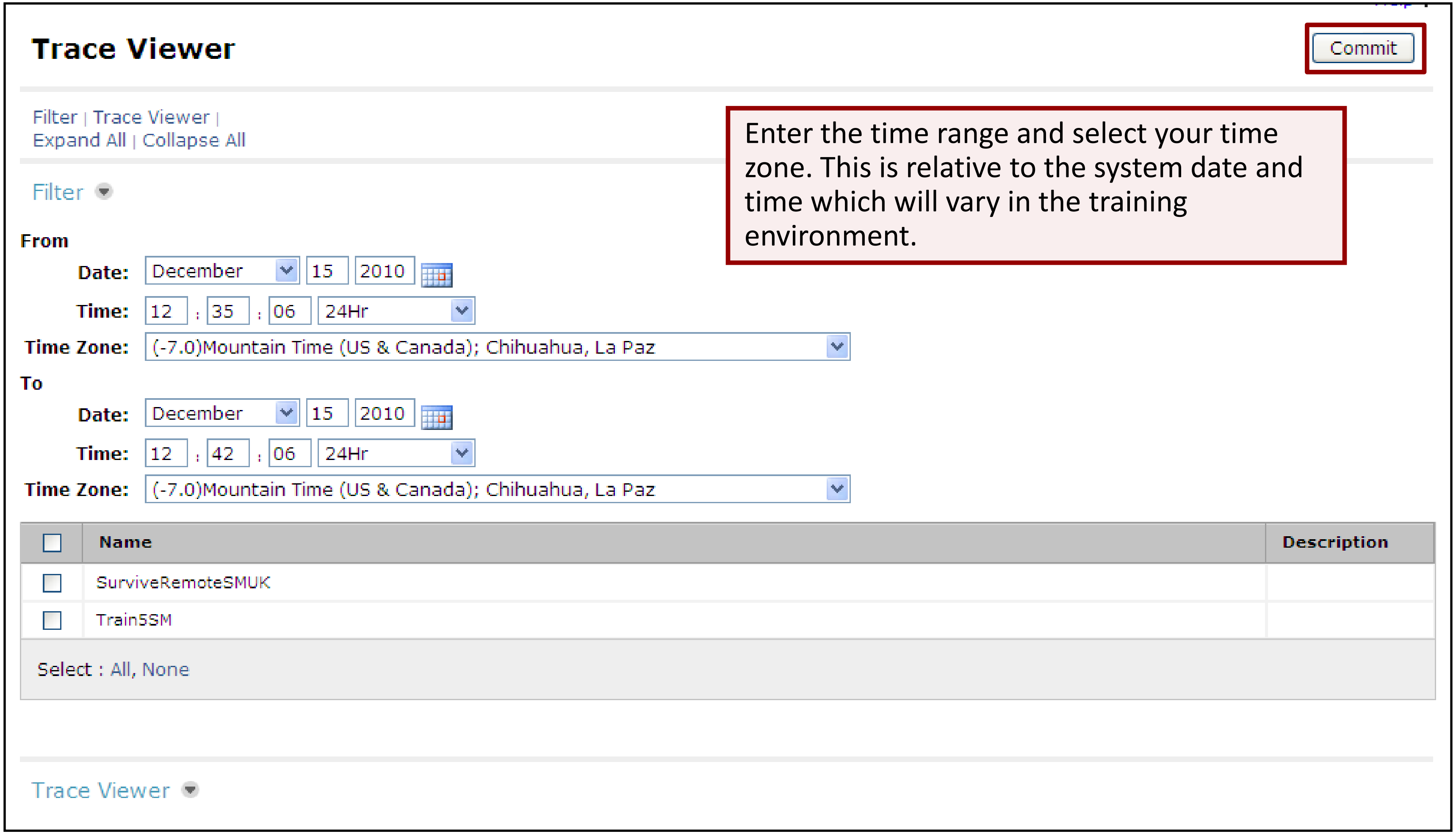
Filter: Enable

	Details	Time	Tracing Entity	From	Action	To	Protocol	Call ID

*Required

Commit

Viewing the SIP Trace - Filter



From

Date: December 15 2010

Time: 12 : 35 : 06 24Hr

Time Zone: (-7.0)Mountain Time (US & Canada); Chihuahua, La Paz

To

Date: December 15 2010

Time: 12 : 42 : 06 24Hr

Time Zone: (-7.0)Mountain Time (US & Canada); Chihuahua, La Paz

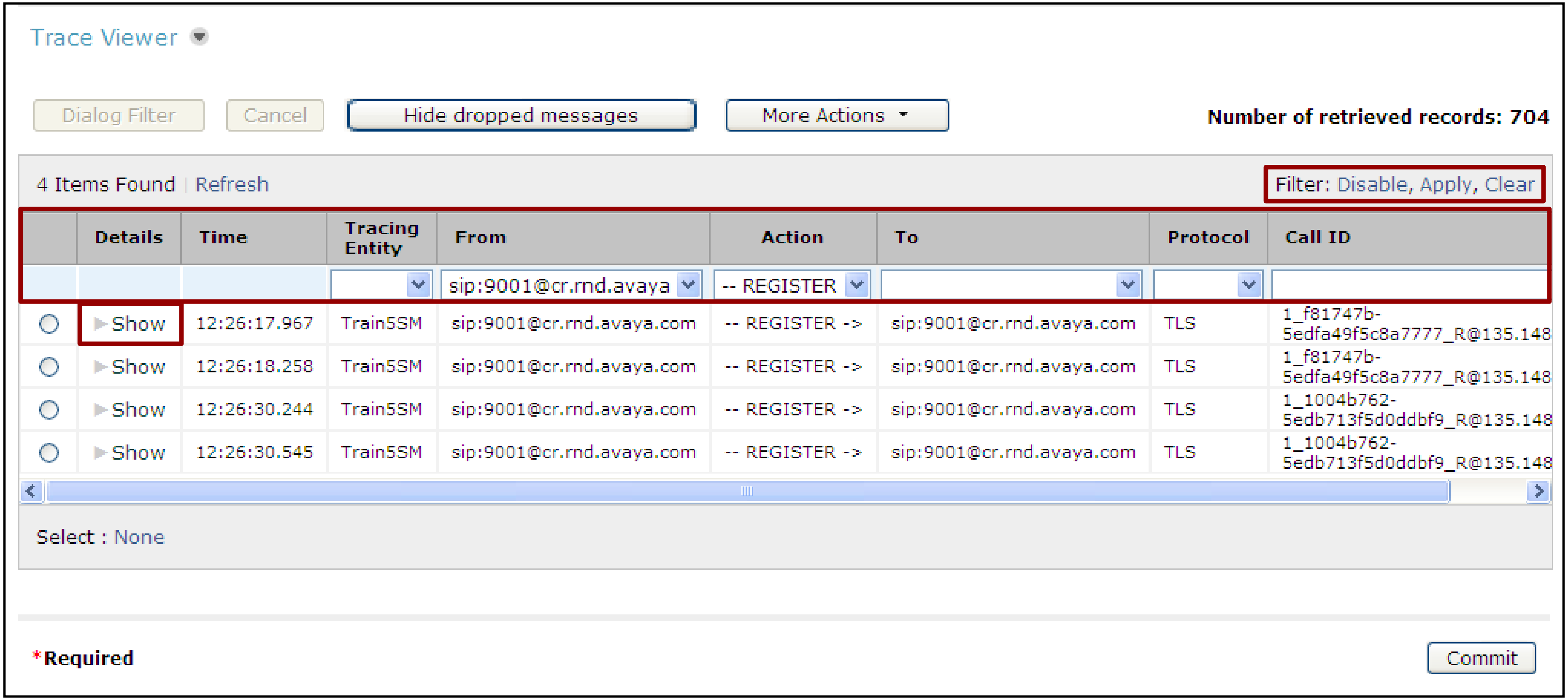
□	Name	Description
□	SurviveRemoteSMUK	
□	Train5SM	

Select : All, None

Enter the time range and select your time zone. This is relative to the system date and time which will vary in the training environment.

Viewing the SIP Trace

Lots and Lots of Messages – enable filter of results



Number of retrieved records: 704

4 Items Found | Refresh

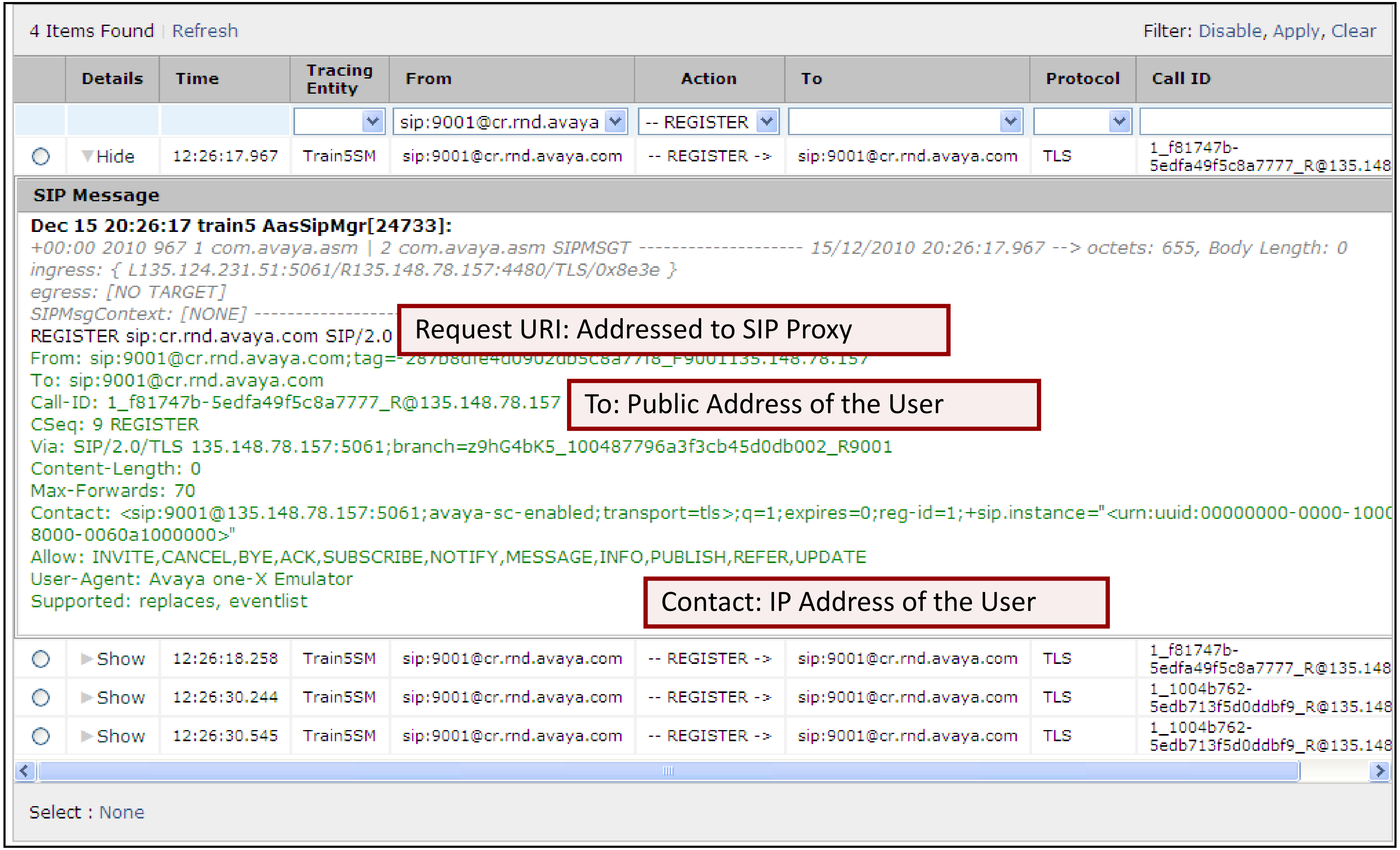
Filter: Disable, Apply, Clear

	Details	Time	Tracing Entity	From	Action	To	Protocol	Call ID
				sip:9001@cr.rnd.avaya	-- REGISTER			
○	▶ Show	12:26:17.967	Train5SM	sip:9001@cr.rnd.avaya.com	-- REGISTER ->	sip:9001@cr.rnd.avaya.com	TLS	1_f81747b-5edfa49f5c8a7777_R@135.148
○	▶ Show	12:26:18.258	Train5SM	sip:9001@cr.rnd.avaya.com	-- REGISTER ->	sip:9001@cr.rnd.avaya.com	TLS	1_f81747b-5edfa49f5c8a7777_R@135.148
○	▶ Show	12:26:30.244	Train5SM	sip:9001@cr.rnd.avaya.com	-- REGISTER ->	sip:9001@cr.rnd.avaya.com	TLS	1_1004b762-5edb713f5d0ddbf9_R@135.148
○	▶ Show	12:26:30.545	Train5SM	sip:9001@cr.rnd.avaya.com	-- REGISTER ->	sip:9001@cr.rnd.avaya.com	TLS	1_1004b762-5edb713f5d0ddbf9_R@135.148

Select : None

*Required

View a SIP Message



4 Items Found | Refresh

Filter: Disable, Apply, Clear

	Details	Time	Tracing Entity	From	Action	To	Protocol	Call ID
				sip:9001@cr.rnd.avaya	-- REGISTER			
○	▼Hide	12:26:17.967	Train5SM	sip:9001@cr.rnd.avaya.com	-- REGISTER ->	sip:9001@cr.rnd.avaya.com	TLS	1_f81747b- 5edfa49f5c8a7777_R@135.148

SIP Message

```
Dec 15 20:26:17 train5 AasSipMgr[24733]:
+00:00 2010 967 1 com.avaya.asm | 2 com.avaya.asm SIPMSGT ------------------- 15/12/2010 20:26:17.967 --> octets: 655, Body Length: 0
ingress: { L135.124.231.51:5061/R135.148.78.157:4480/TLS/0x8e3e }
egress: [NO TARGET]
SIPMsgContext: [NONE] ----------------
REGISTER sip:cr.rnd.avaya.com SIP/2.0
From: sip:9001@cr.rnd.avaya.com;tag=287b8dfe4d0902db5c8a7718_F9001135.148.78.157
To: sip:9001@cr.rnd.avaya.com
Call-ID: 1_f81747b-5edfa49f5c8a7777_R@135.148.78.157
CSeq: 9 REGISTER
Via: SIP/2.0/TLS 135.148.78.157:5061;branch=z9hG4bK5_100487796a3f3cb45d0db002_R9001
Content-Length: 0
Max-Forwards: 70
Contact: <sip:9001@135.148.78.157:5061;avaya-sc-enabled;transport=tls>;q=1;expires=0;reg-id=1;+sip.instance="<urn:uuid:00000000-0000-1000
8000-0060a1000000>"
Allow: INVITE,CANCEL,BYE,ACK,SUBSCRIBE,NOTIFY,MESSAGE,INFO,PUBLISH,REFER,UPDATE
User-Agent: Avaya one-X Emulator
Supported: replaces, eventlist
```

Request URI: Addressed to SIP Proxy

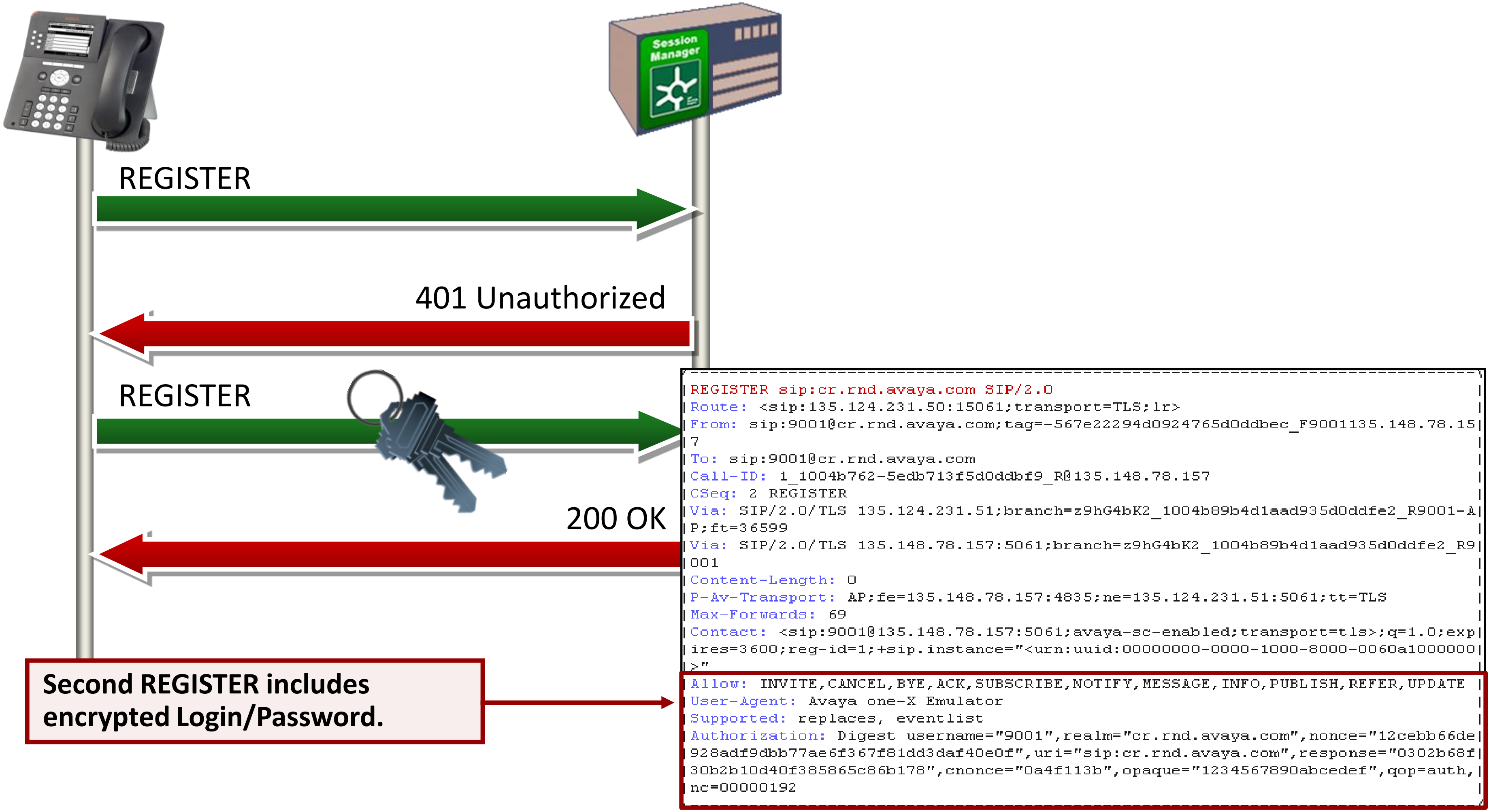
To: Public Address of the User

Contact: IP Address of the User

○	▶Show	12:26:18.258	Train5SM	sip:9001@cr.rnd.avaya.com	-- REGISTER ->	sip:9001@cr.rnd.avaya.com	TLS	1_f81747b- 5edfa49f5c8a7777_R@135.148
○	▶Show	12:26:30.244	Train5SM	sip:9001@cr.rnd.avaya.com	-- REGISTER ->	sip:9001@cr.rnd.avaya.com	TLS	1_1004b762- 5edb713f5d0ddbf9_R@135.148
○	▶Show	12:26:30.545	Train5SM	sip:9001@cr.rnd.avaya.com	-- REGISTER ->	sip:9001@cr.rnd.avaya.com	TLS	1_1004b762- 5edb713f5d0ddbf9_R@135.148

Select : None

Sample Registration Trace

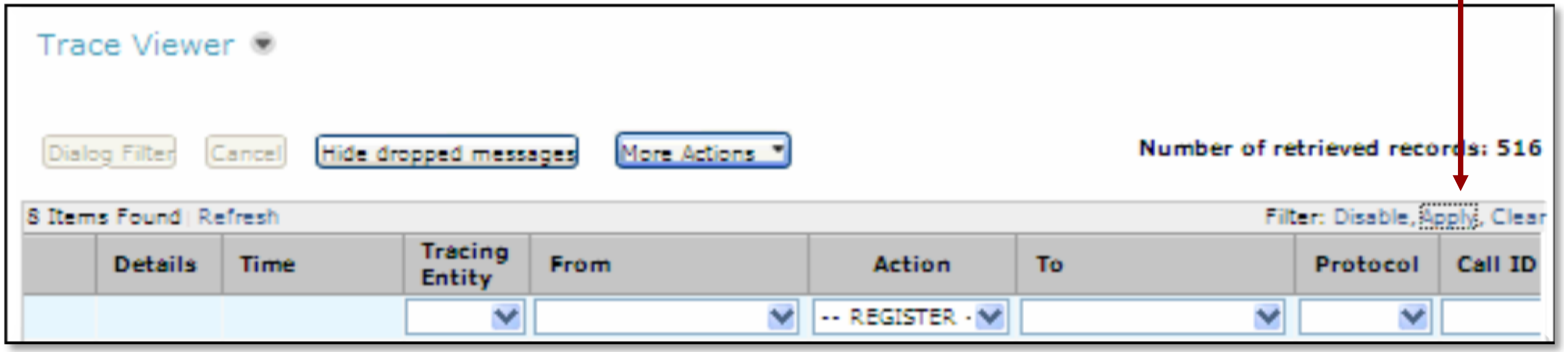


```
REGISTER sip:cr.rnd.avaya.com SIP/2.0
Route: <sip:135.124.231.50:15061;transport=TLS;lr>
From: sip:9001@cr.rnd.avaya.com;tag=-567e22294d0924765d0ddbec_F9001135.148.78.15
7
To: sip:9001@cr.rnd.avaya.com
Call-ID: 1_1004b762-5edb713f5d0ddbf9_R@135.148.78.157
CSeq: 2 REGISTER
Via: SIP/2.0/TLS 135.124.231.51;branch=z9hG4bK2_1004b89b4d1aad935d0ddfe2_R9001-A
P;ft=36599
Via: SIP/2.0/TLS 135.148.78.157:5061;branch=z9hG4bK2_1004b89b4d1aad935d0ddfe2_R9
001
Content-Length: 0
P-Av-Transport: AP;fe=135.148.78.157:4835;ne=135.124.231.51:5061;tt=TLS
Max-Forwards: 69
Contact: <sip:9001@135.148.78.157:5061;avaya-sc-enabled;transport=tls>;q=1.0;exp
ires=3600;reg-id=1;+sip.instance="<urn:uuid:00000000-0000-1000-8000-0060a1000000
>"
Allow: INVITE,CANCEL,BYE,ACK,SUBSCRIBE,NOTIFY,MESSAGE,INFO,PUBLISH,REFER,UPDATE
User-Agent: Avaya one-X Emulator
Supported: replaces, eventlist
Authorization: Digest username="9001",realm="cr.rnd.avaya.com",nonce="12cebb66de
928adf9dbb77ae6f367f81dd3daf40e0f",uri="sip:cr.rnd.avaya.com",response="0302b68f
30b2b10d40f385865c86b178",cnonce="0a4f113b",opaque="1234567890abcedef",qop=auth,
nc=00000192
```

Second REGISTER includes encrypted Login/Password.

Exercise: View SIP Trace Viewer

Step	Action
1	Navigate from the System Manager Home Page to Session Manager >> System Tools >> SIP Tracer Viewer
2	**Enable** the Filter in Results to display **REGISTER**
3	Select your ASM from the drop-down menu.
4	Select **REGISTER** in Actions column
5	Select Apply

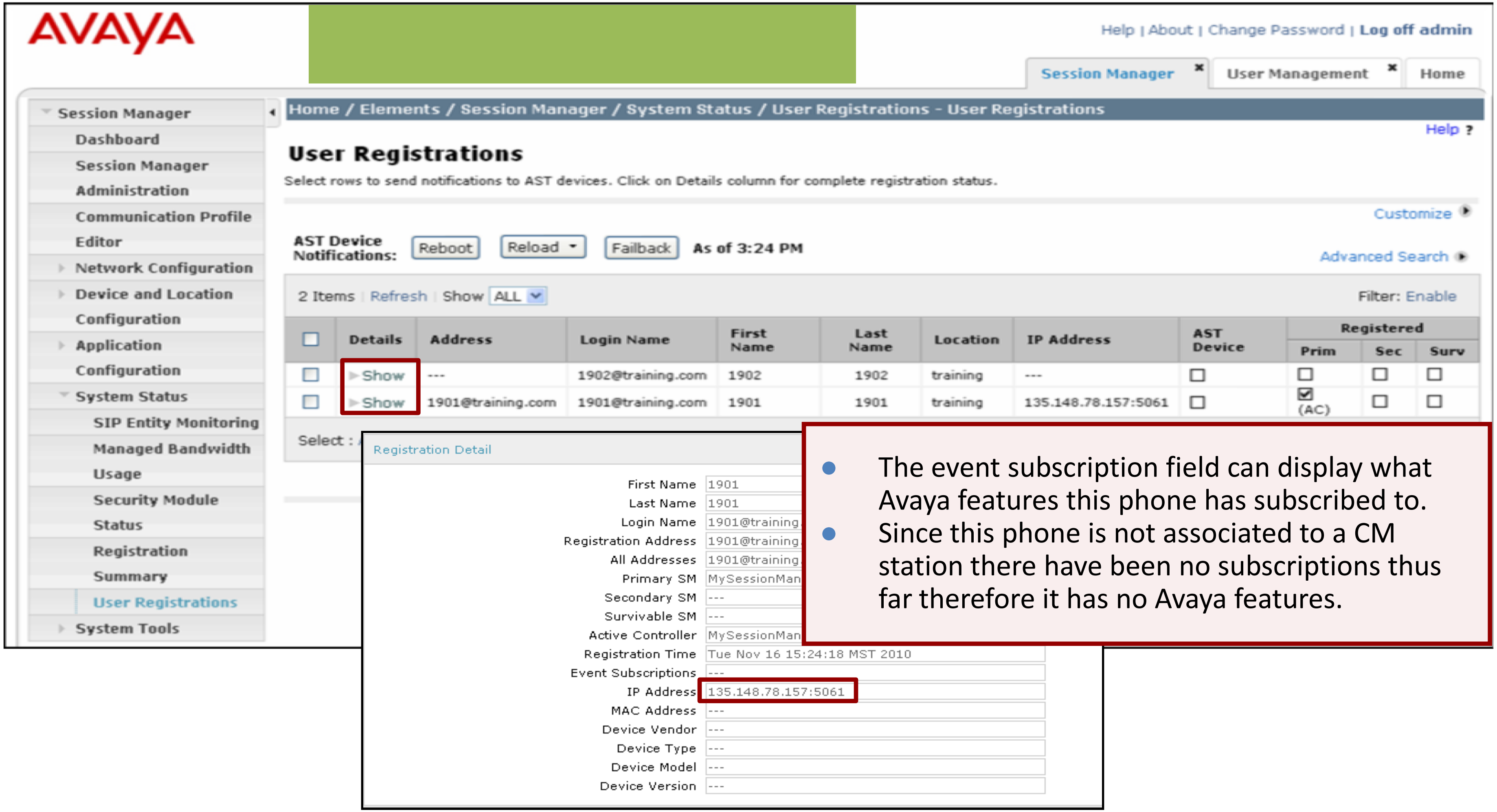


Number of retrieved records: 516

8 Items Found

	Details	Time	Tracing Entity	From	Action	To	Protocol	Call ID
					-- REGISTER -			

User Registrations



Home / Elements / Session Manager / System Status / User Registrations - User Registrations

User Registrations

Select rows to send notifications to AST devices. Click on Details column for complete registration status.

AST Device Notifications: Reboot Reload Failback As of 3:24 PM

2 Items | Refresh | Show ALL

□	Details	Address	Login Name	First Name	Last Name	Location	IP Address	AST Device	Registered		
									Prim	Sec	Surv
□	▸ Show	---	1902@training.com	1902	1902	training	---	□	□	□	□
□	▸ Show	1901@training.com	1901@training.com	1901	1901	training	135.148.78.157:5061	□	☑ (AC)	□	□

Select :

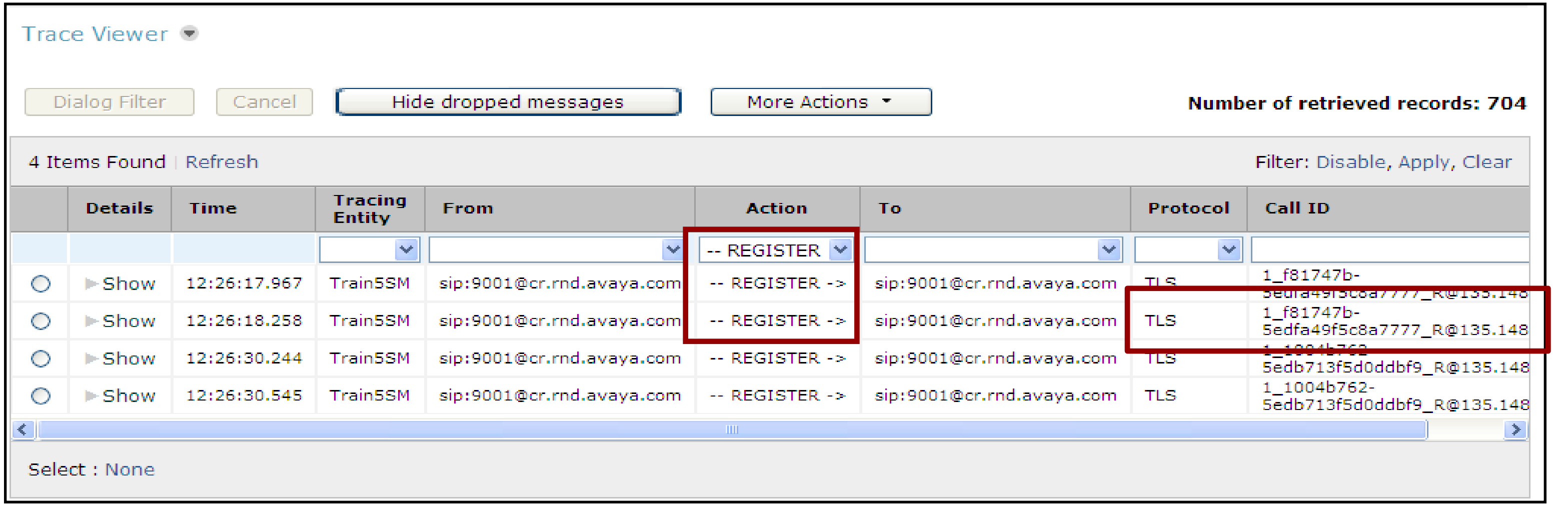
Registration Detail

First Name	1901
Last Name	1901
Login Name	1901@training
Registration Address	1901@training
All Addresses	1901@training
Primary SM	MySessionMan
Secondary SM	---
Survivable SM	---
Active Controller	MySessionMan
Registration Time	Tue Nov 16 15:24:18 MST 2010
Event Subscriptions	---
IP Address	135.148.78.157:5061
MAC Address	---
Device Vendor	---
Device Type	---
Device Model	---
Device Version	---

- The event subscription field can display what Avaya features this phone has subscribed to.
- Since this phone is not associated to a CM station there have been no subscriptions thus far therefore it has no Avaya features.

Exercise: View User Registrations

Step	Action
1	Navigate from the System Manager Home Page to Session Manager >> System Tools >> SIP Tracer Viewer
2	**Enable** the Filter in Results to display **REGISTER**
3	Select your ASM from the drop-down menu.
4	Select **REGISTER** in Actions column



Trace Viewer

Number of retrieved records: 704

4 Items Found | Refresh

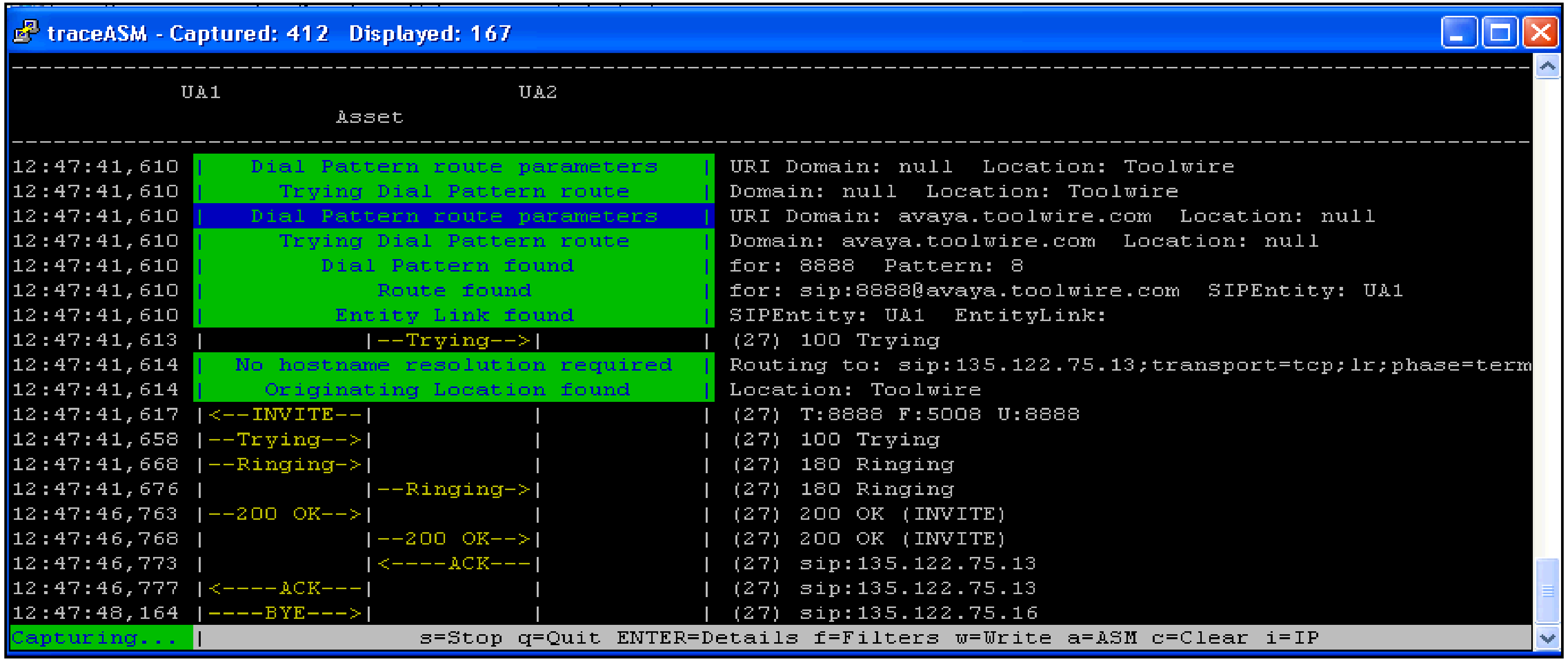
Filter: Disable, Apply, Clear

	Details	Time	Tracing Entity	From	Action	To	Protocol	Call ID
					-- REGISTER			
○	▶ Show	12:26:17.967	Train5SM	sip:9001@cr.rnd.avaya.com	-- REGISTER ->	sip:9001@cr.rnd.avaya.com	TLS	1_f81747b-5edfa49f5c8a7777_R@135.148
○	▶ Show	12:26:18.258	Train5SM	sip:9001@cr.rnd.avaya.com	-- REGISTER ->	sip:9001@cr.rnd.avaya.com	TLS	1_f81747b-5edfa49f5c8a7777_R@135.148
○	▶ Show	12:26:30.244	Train5SM	sip:9001@cr.rnd.avaya.com	-- REGISTER ->	sip:9001@cr.rnd.avaya.com	TLS	1_1004b762-5edb713f5d0ddbf9_R@135.148
○	▶ Show	12:26:30.545	Train5SM	sip:9001@cr.rnd.avaya.com	-- REGISTER ->	sip:9001@cr.rnd.avaya.com	TLS	1_1004b762-5edb713f5d0ddbf9_R@135.148

Select : None

Alternate SIP Tracing - Analysing the Registration

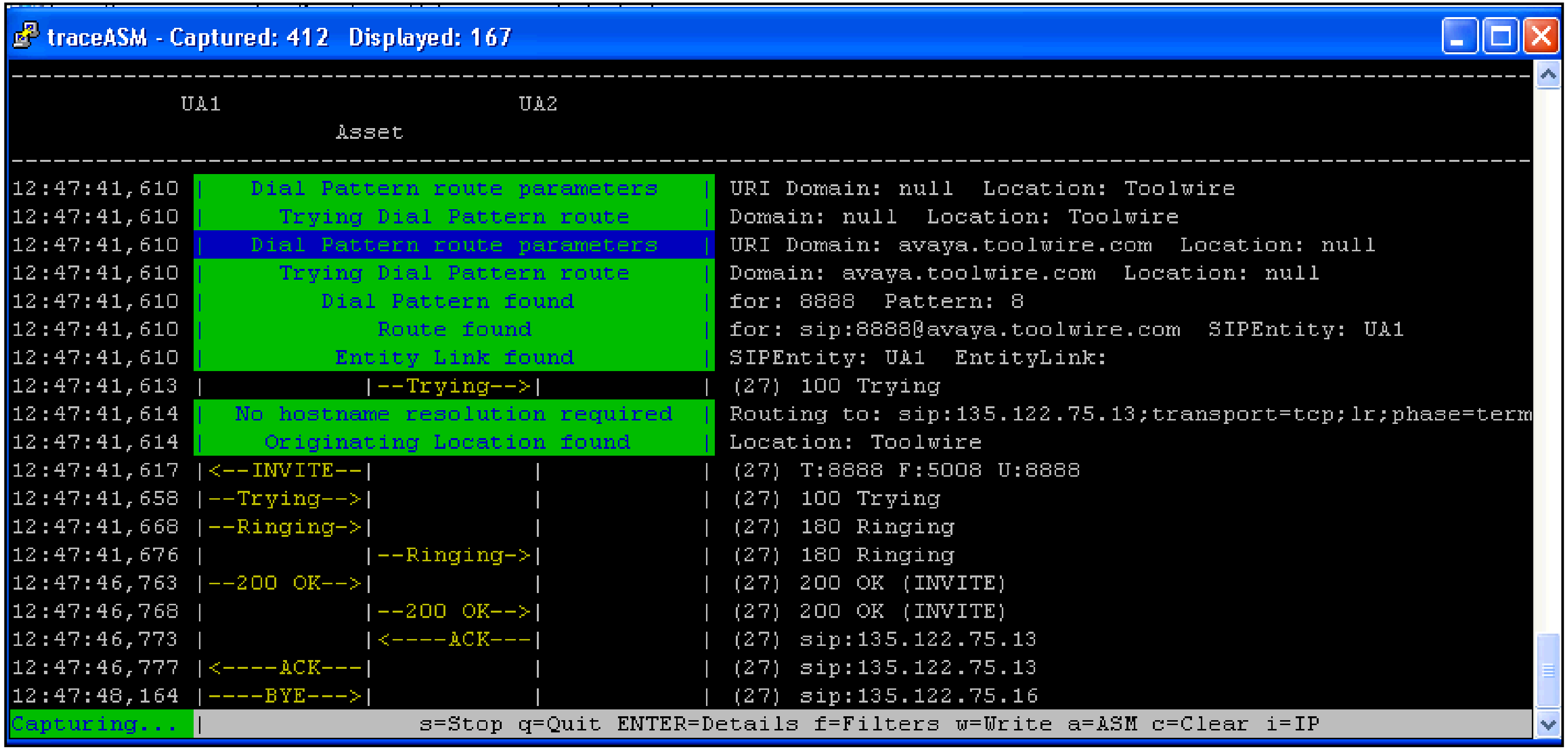
- The traceSM tool shows the SIP call flow for the Session Manager
- It also gives insight into ASM decisions



```
---------------------------------------------------------------------------------------------------------
            UA1                      UA2
                       Asset
---------------------------------------------------------------------------------------------------------
12:47:41,610 |  Dial Pattern route parameters  | URI Domain: null  Location: Toolwire
12:47:41,610 |    Trying Dial Pattern route    | Domain: null  Location: Toolwire
12:47:41,610 |  Dial Pattern route parameters  | URI Domain: avaya.toolwire.com  Location: null
12:47:41,610 |    Trying Dial Pattern route    | Domain: avaya.toolwire.com  Location: null
12:47:41,610 |       Dial Pattern found        | for: 8888  Pattern: 8
12:47:41,610 |           Route found           | for: sip:8888@avaya.toolwire.com  SIPEntity: UA1
12:47:41,610 |        Entity Link found        | SIPEntity: UA1  EntityLink:
12:47:41,613 |           |--Trying-->|         | (27) 100 Trying
12:47:41,614 |  No hostname resolution required | Routing to: sip:135.122.75.13;transport=tcp;lr;phase=term
12:47:41,614 |   Originating Location found    | Location: Toolwire
12:47:41,617 |<--INVITE--|           |         | (27) T:8888 F:5008 U:8888
12:47:41,658 |--Trying-->|           |         | (27) 100 Trying
12:47:41,668 |--Ringing->|           |         | (27) 180 Ringing
12:47:41,676 |           |--Ringing->|         | (27) 180 Ringing
12:47:46,763 |--200 OK-->|           |         | (27) 200 OK (INVITE)
12:47:46,768 |           |--200 OK-->|         | (27) 200 OK (INVITE)
12:47:46,773 |           |<----ACK---|         | (27) sip:135.122.75.13
12:47:46,777 |<----ACK---|           |         | (27) sip:135.122.75.13
12:47:48,164 |----BYE--->|           |         | (27) sip:135.122.75.16
Capturing... |        s=Stop q=Quit ENTER=Details f=Filters w=Write a=ASM c=Clear i=IP
```

traceSM Demo-navigating through call flow

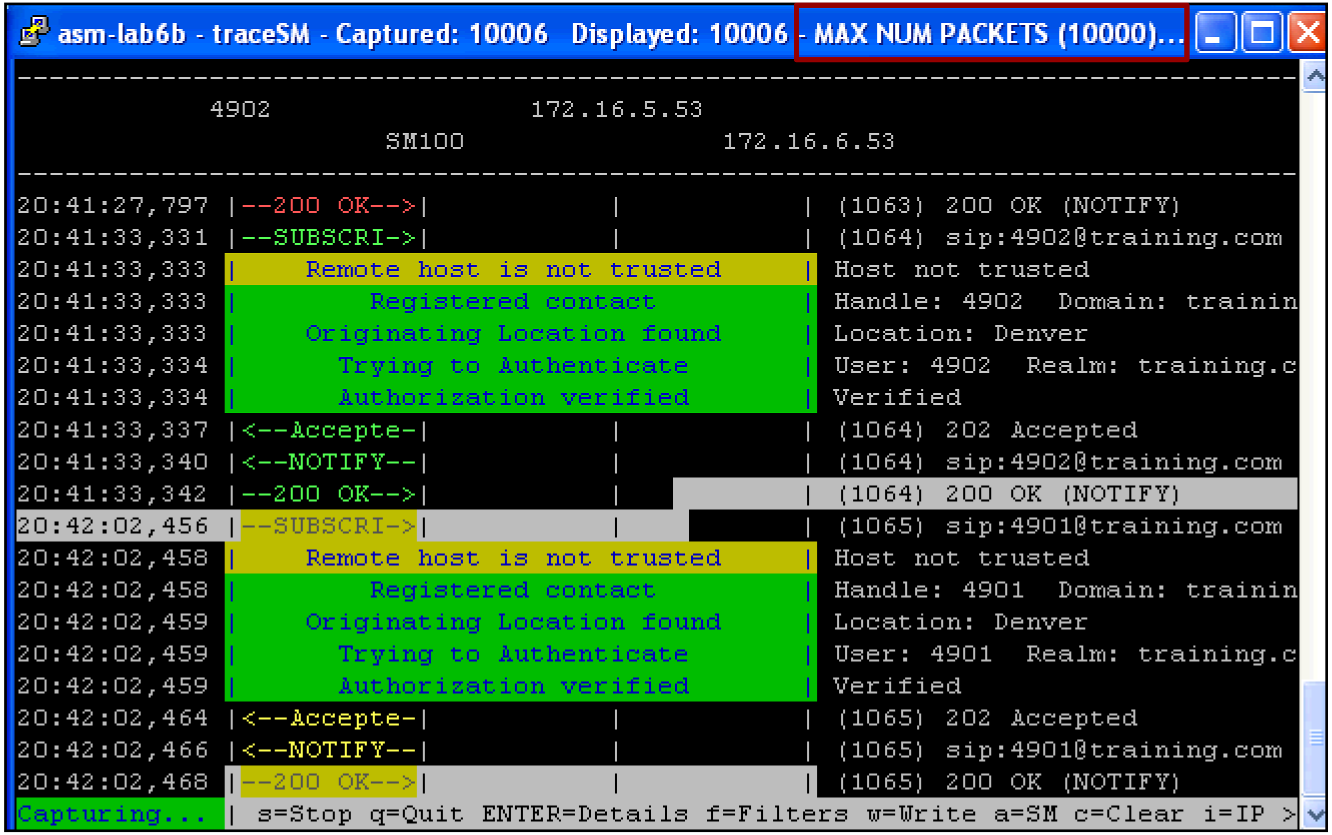
- Select the colored area with your mouse
- Use the up ↑ and down ↓ arrows on your keyboard to navigate through the call flow
- Select “enter” to look at the details of the SIP message



```
----------------------------------------------------------------------------------------------------------
            UA1                     UA2
                       Asset
----------------------------------------------------------------------------------------------------------
12:47:41,610 |    Dial Pattern route parameters    | URI Domain: null  Location: Toolwire
12:47:41,610 |      Trying Dial Pattern route      | Domain: null  Location: Toolwire
12:47:41,610 |    Dial Pattern route parameters    | URI Domain: avaya.toolwire.com  Location: null
12:47:41,610 |      Trying Dial Pattern route      | Domain: avaya.toolwire.com  Location: null
12:47:41,610 |         Dial Pattern found          | for: 8888  Pattern: 8
12:47:41,610 |             Route found             | for: sip:8888@avaya.toolwire.com  SIPEntity: UA1
12:47:41,610 |          Entity Link found          | SIPEntity: UA1  EntityLink:
12:47:41,613 |           |--Trying-->|             | (27) 100 Trying
12:47:41,614 |   No hostname resolution required   | Routing to: sip:135.122.75.13;transport=tcp;lr;phase=term
12:47:41,614 |     Originating Location found      | Location: Toolwire
12:47:41,617 |<--INVITE--|           |             | (27) T:8888 F:5008 U:8888
12:47:41,658 |--Trying-->|           |             | (27) 100 Trying
12:47:41,668 |--Ringing->|           |             | (27) 180 Ringing
12:47:41,676 |           |--Ringing->|             | (27) 180 Ringing
12:47:46,763 |--200 OK-->|           |             | (27) 200 OK (INVITE)
12:47:46,768 |           |--200 OK-->|             | (27) 200 OK (INVITE)
12:47:46,773 |           |<----ACK---|             | (27) sip:135.122.75.13
12:47:46,777 |<----ACK---|           |             | (27) sip:135.122.75.13
12:47:48,164 |----BYE--->|           |             | (27) sip:135.122.75.16
Capturing... |          s=Stop q=Quit ENTER=Details f=Filters w=Write a=ASM c=Clear i=IP
```

traceSM

- traceSM will capture a maximum of approximately10,000 packets.
- It opens a new log file once it reaches its limit.



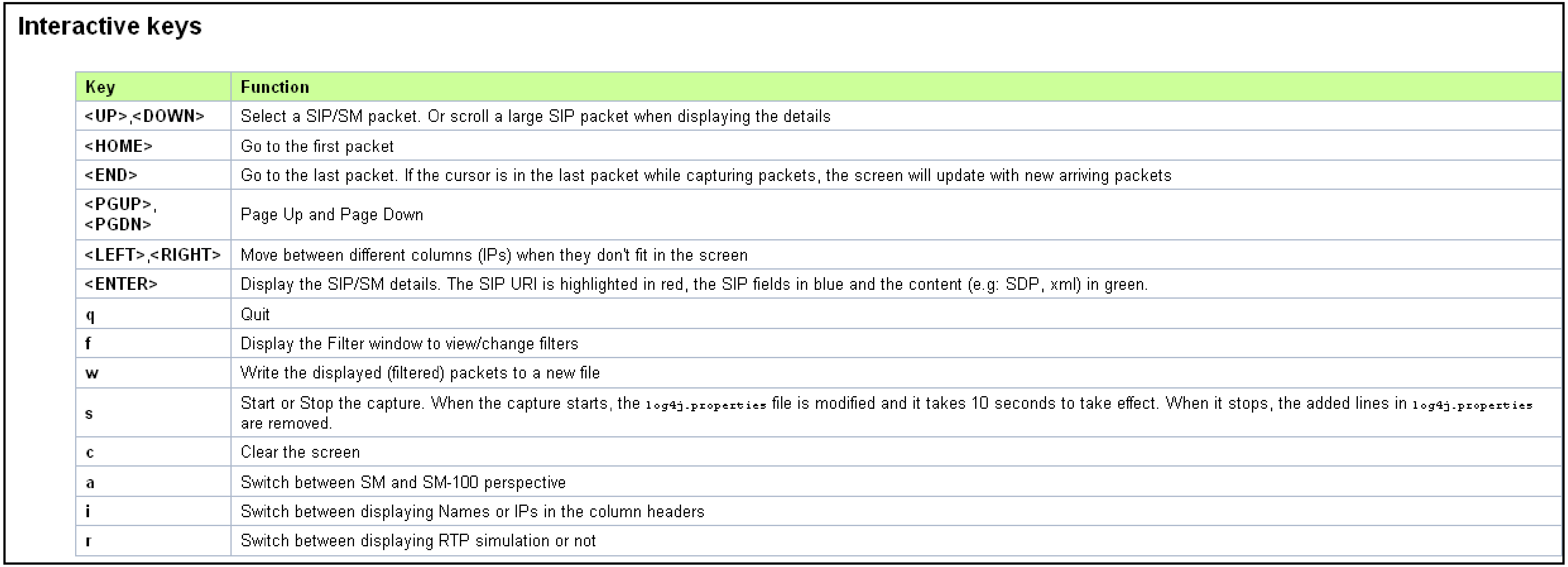
asm-lab6b - traceSM - Captured: 10006   Displayed: 10006 - MAX NUM PACKETS (10000)...

```
------------------------------------------------------------------------------------
            4902                  172.16.5.53
                       SM100                  172.16.6.53
------------------------------------------------------------------------------------
20:41:27,797 |--200 OK-->|           |           | (1063) 200 OK (NOTIFY)
20:41:33,331 |--SUBSCRI->|           |           | (1064) sip:4902@training.com
20:41:33,333 |    Remote host is not trusted     | Host not trusted
20:41:33,333 |        Registered contact         | Handle: 4902   Domain: trainin
20:41:33,333 |    Originating Location found     | Location: Denver
20:41:33,334 |      Trying to Authenticate       | User: 4902   Realm: training.c
20:41:33,334 |      Authorization verified       | Verified
20:41:33,337 |<--Accepte-|           |           | (1064) 202 Accepted
20:41:33,340 |<--NOTIFY--|           |           | (1064) sip:4902@training.com
20:41:33,342 |--200 OK-->|           |           | (1064) 200 OK (NOTIFY)
20:42:02,456 |--SUBSCRI->|           |           | (1065) sip:4901@training.com
20:42:02,458 |    Remote host is not trusted     | Host not trusted
20:42:02,458 |        Registered contact         | Handle: 4901   Domain: trainin
20:42:02,459 |    Originating Location found     | Location: Denver
20:42:02,459 |      Trying to Authenticate       | User: 4901   Realm: training.c
20:42:02,459 |      Authorization verified       | Verified
20:42:02,464 |<--Accepte-|           |           | (1065) 202 Accepted
20:42:02,466 |<--NOTIFY--|           |           | (1065) sip:4901@training.com
20:42:02,468 |--200 OK-->|           |           | (1065) 200 OK (NOTIFY)
Capturing... | s=Stop q=Quit ENTER=Details f=Filters w=Write a=SM c=Clear i=IP >
```

traceSM - SIP Tracing

traceSM

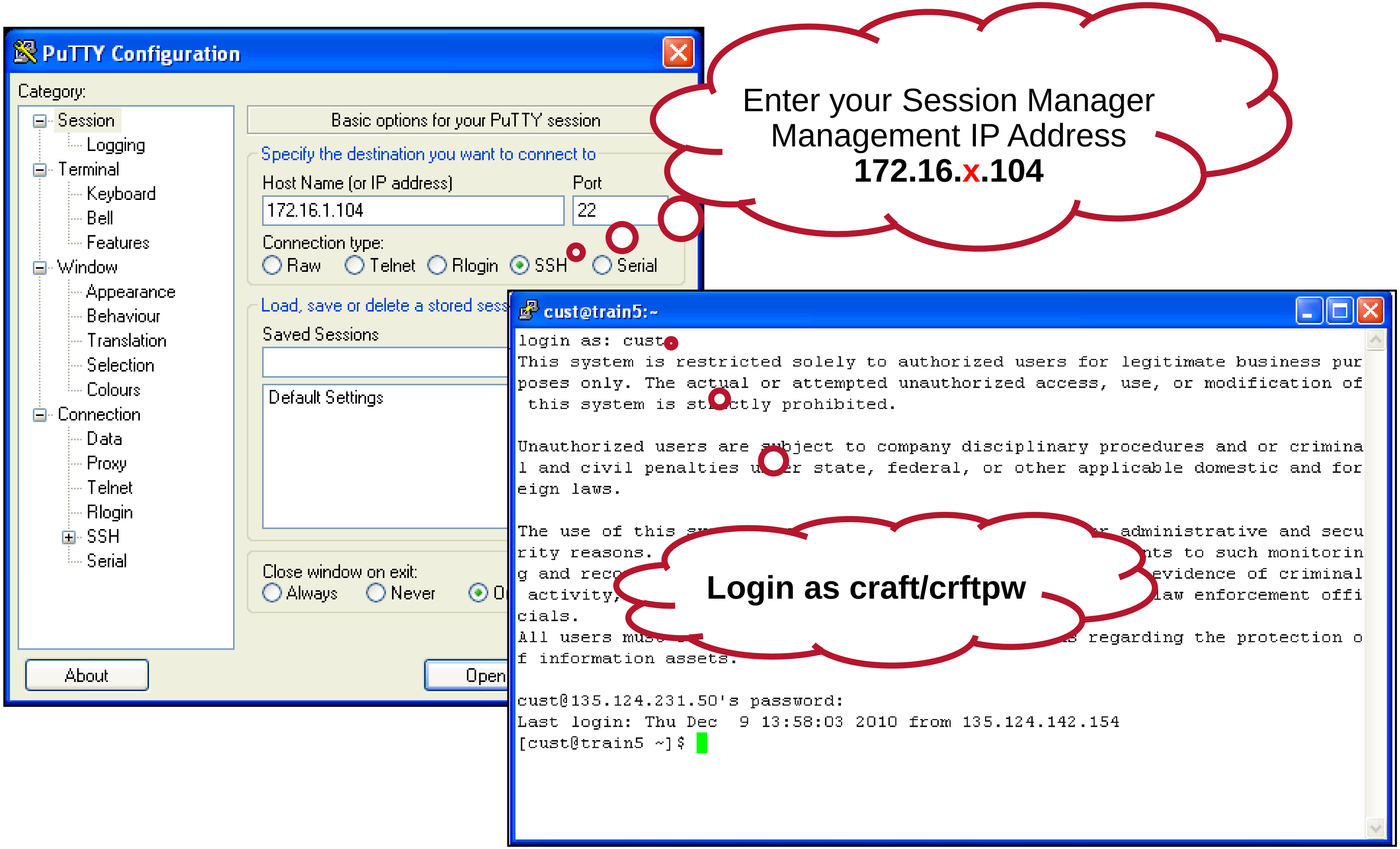
- Run traceSM -h to get the help with the different arguments that the script supports.



Interactive keys

Key	Function
<UP>,<DOWN>	Select a SIP/SM packet. Or scroll a large SIP packet when displaying the details
<HOME>	Go to the first packet
<END>	Go to the last packet. If the cursor is in the last packet while capturing packets, the screen will update with new arriving packets
<PGUP>, <PGDN>	Page Up and Page Down
<LEFT>,<RIGHT>	Move between different columns (IPs) when they don't fit in the screen
<ENTER>	Display the SIP/SM details. The SIP URI is highlighted in red, the SIP fields in blue and the content (e.g: SDP, xml) in green.
q	Quit
f	Display the Filter window to view/change filters
w	Write the displayed (filtered) packets to a new file
s	Start or Stop the capture. When the capture starts, the log4j.properties file is modified and it takes 10 seconds to take effect. When it stops, the added lines in log4j.properties are removed.
c	Clear the screen
a	Switch between SM and SM-100 perspective
i	Switch between displaying Names or IPs in the column headers
r	Switch between displaying RTP simulation or not

traceSM – SSH Access to Session Manager



Specify the destination you want to connect to

Host Name (or IP address): 172.16.1.104

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● O

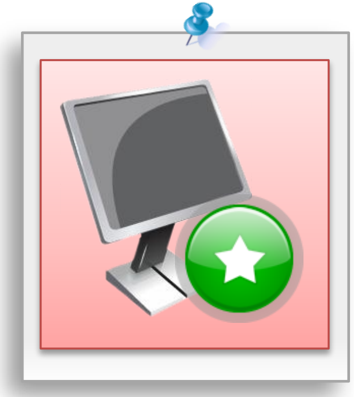
```
login as: cust
This system is restricted solely to authorized users for legitimate business pur
poses only. The actual or attempted unauthorized access, use, or modification of
 this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or crimina
l and civil penalties under state, federal, or other applicable domestic and for
eign laws.

The use of this sy                                   r administrative and secu
rity reasons.                                          nts to such monitorin
g and reco                                              evidence of criminal
 activity,                                               law enforcement offi
cials.
All users mus                                      s regarding the protection o
f information assets.

cust@135.124.231.50's password:
Last login: Thu Dec  9 13:58:03 2010 from 135.124.142.154
[cust@train5 ~]$
```

Enter your Session Manager Management IP Address **172.16.x.104**

Login as craft/crftpw

Exercise: Run traceSM

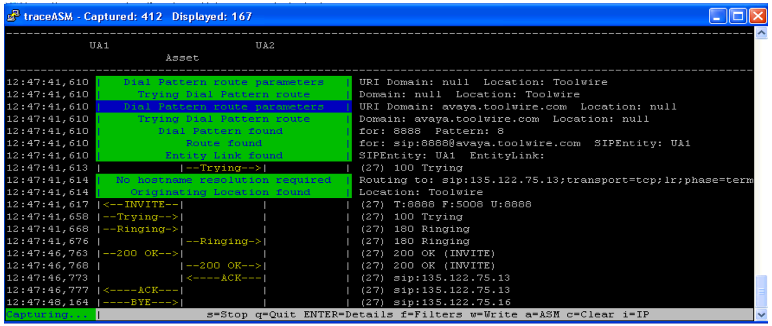
Step	Action
1	Connect to Session Manager using Putty IP Address: **172.16.x.104**
2	Login: **craft** password: **crftpw**
3	At command line type: **traceSM –x**
4	Type ‘**s**’ to start the capture
5	Place the previous call again



TIPS

- Use your up/down arrow keys to select a line in the trace
- Press ‘Enter’ to view the details of a selected line
- Press ‘Enter’ to close details of selected line
- ‘c’ will clear the capture screen
- ‘s’ to stop the capture once finished.
- ‘q’ to exit the tool
- ‘f’ to apply a filter
- traceSM –h for help commands

TraceSM is delivered under /opt/Avaya/contrib/bin



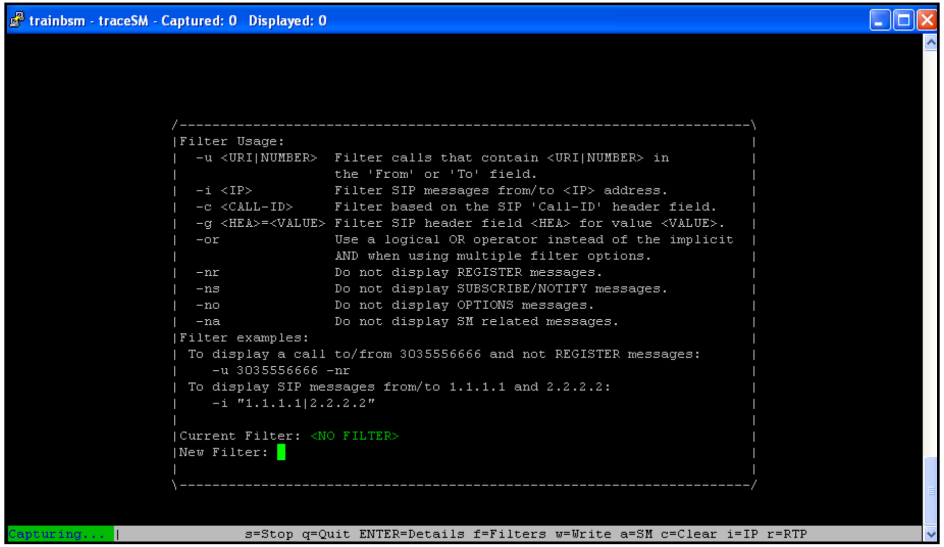
traceASM - Captured: 412 Displayed: 167

```
-------------------------------------------------------------------------------------------------
           UA1                     UA2
                      Asset
-------------------------------------------------------------------------------------------------
12:47:41,610 |   Dial Pattern route parameters   | URI Domain: null  Location: Toolwire
12:47:41,610 |     Trying Dial Pattern route     | Domain: null  Location: Toolwire
12:47:41,610 |   Dial Pattern route parameters   | URI Domain: avaya.toolwire.com  Location: null
12:47:41,610 |     Trying Dial Pattern route     | Domain: avaya.toolwire.com  Location: null
12:47:41,610 |        Dial Pattern found         | for: 8888  Pattern: 8
12:47:41,610 |            Route found            | for: sip:8888@avaya.toolwire.com  SIPEntity: UA1
12:47:41,610 |         Entity Link found         | SIPEntity: UA1  EntityLink:
12:47:41,613 |           |--Trying-->|           | (27) 100 Trying
12:47:41,614 |  No hostname resolution required  | Routing to: sip:135.122.75.13;transport=tcp;lr;phase=term
12:47:41,614 |    Originating Location found     | Location: Toolwire
12:47:41,617 |<--INVITE--|           |           | (27) T:8888 F:5008 U:8888
12:47:41,658 |--Trying-->|           |           | (27) 100 Trying
12:47:41,668 |--Ringing->|           |           | (27) 180 Ringing
12:47:41,676 |           |--Ringing->|           | (27) 180 Ringing
12:47:46,763 |--200 OK-->|           |           | (27) 200 OK (INVITE)
12:47:46,768 |           |--200 OK-->|           | (27) 200 OK (INVITE)
12:47:46,773 |           |<----ACK---|           | (27) sip:135.122.75.13
12:47:46,777 |<----ACK---|           |           | (27) sip:135.122.75.13
12:47:48,164 |----BYE--->|           |           | (27) sip:135.122.75.16
Capturing... |          s=Stop q=Quit ENTER=Details f=Filters w=Write a=ASM c=Clear i=IP
```

traceSM- display filter

traceSM

- Once traceSM is running, type ‘F’ to apply a filter.
- Examples
  - no = no OPTIONS
  - nr = no REGISTERS
  - ns = no SUBSCRIBES
  - u 1901 will filter calls that contain that URI in the from or to headers
  - You can apply multple filters:
    - **u 1901 –no –ns –nr**
      - The above will show only messages to/from 1901 and hide OPTIONS, SUBSCRIBES and REGISTERS

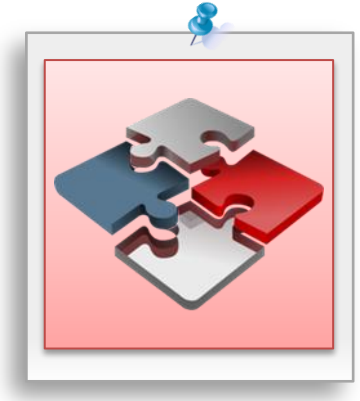


```
/-----------------------------------------------------------------------\
|Filter Usage:                                                          |
|  -u <URI|NUMBER>  Filter calls that contain <URI|NUMBER> in           |
|                   the 'From' or 'To' field.                           |
|  -i <IP>          Filter SIP messages from/to <IP> address.           |
|  -c <CALL-ID>     Filter based on the SIP 'Call-ID' header field.     |
|  -g <HEA>=<VALUE> Filter SIP header field <HEA> for value <VALUE>.    |
|  -or              Use a logical OR operator instead of the implicit   |
|                   AND when using multiple filter options.             |
|  -nr              Do not display REGISTER messages.                   |
|  -ns              Do not display SUBSCRIBE/NOTIFY messages.           |
|  -no              Do not display OPTIONS messages.                    |
|  -na              Do not display SM related messages.                 |
|Filter examples:                                                       |
| To display a call to/from 3035556666 and not REGISTER messages:       |
|    -u 3035556666 -nr                                                  |
| To display SIP messages from/to 1.1.1.1 and 2.2.2.2:                  |
|    -i "1.1.1.1|2.2.2.2"                                               |
|                                                                       |
|Current Filter: <NO FILTER>                                            |
|New Filter:                                                            |
|                                                                       |
\-----------------------------------------------------------------------/
Capturing... |          s=Stop q=Quit ENTER=Details f=Filters w=Write a=SM c=Clear i=IP r=RTP
```

Lesson Summary

You have completed the following lesson objectives:

- Use SIP tracing tools to view the SIP call flow



AVAYA | LEARNING

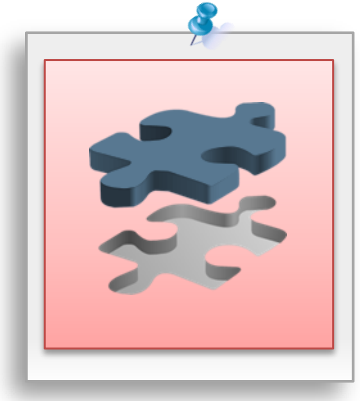
Lesson 4

SIP Registry Routing

Lesson Objective

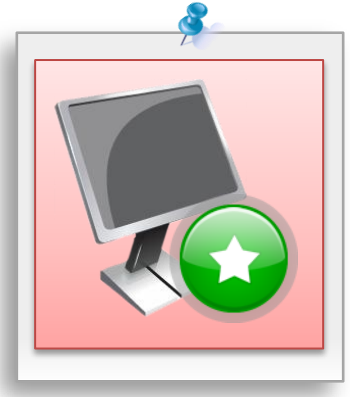
After completing this lesson you will be able to:

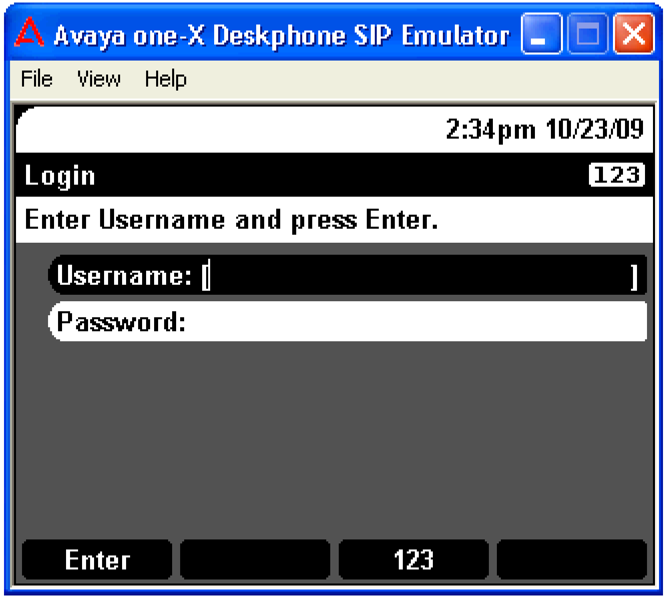
- Examine how Session Manager performs Registry Routing



Exercise: Making a Call

Step	Action
1	Run your two SIP Emulators: x9x1 dials x9x2





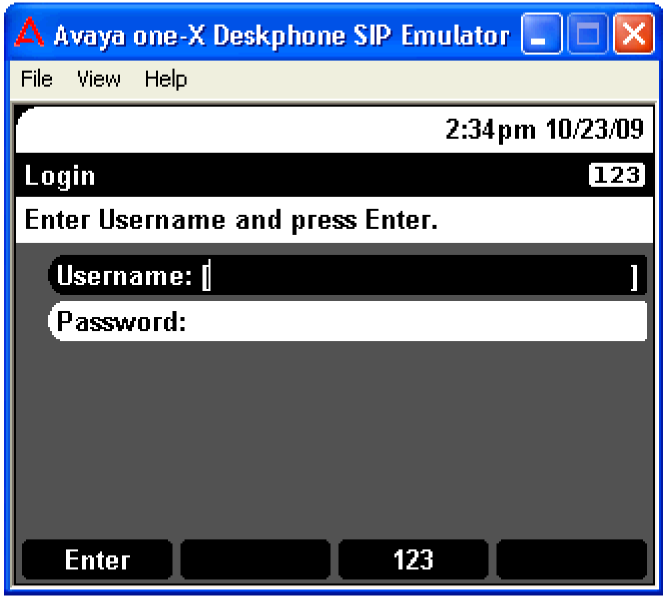
2:34pm 10/23/09

Login 123

Enter Username and press Enter.

Username: [ ]

Password:



2:34pm 10/23/09

Login 123

Enter Username and press Enter.

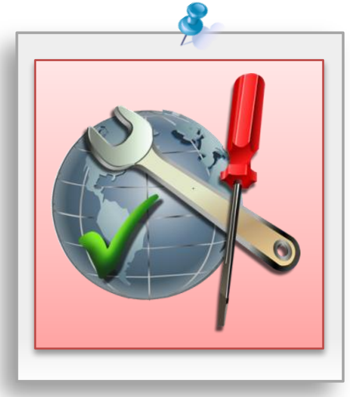
Username: [ ]

Password:

Registry Routing or Routing Policy?

Troubleshooting

Did the call complete successfully?



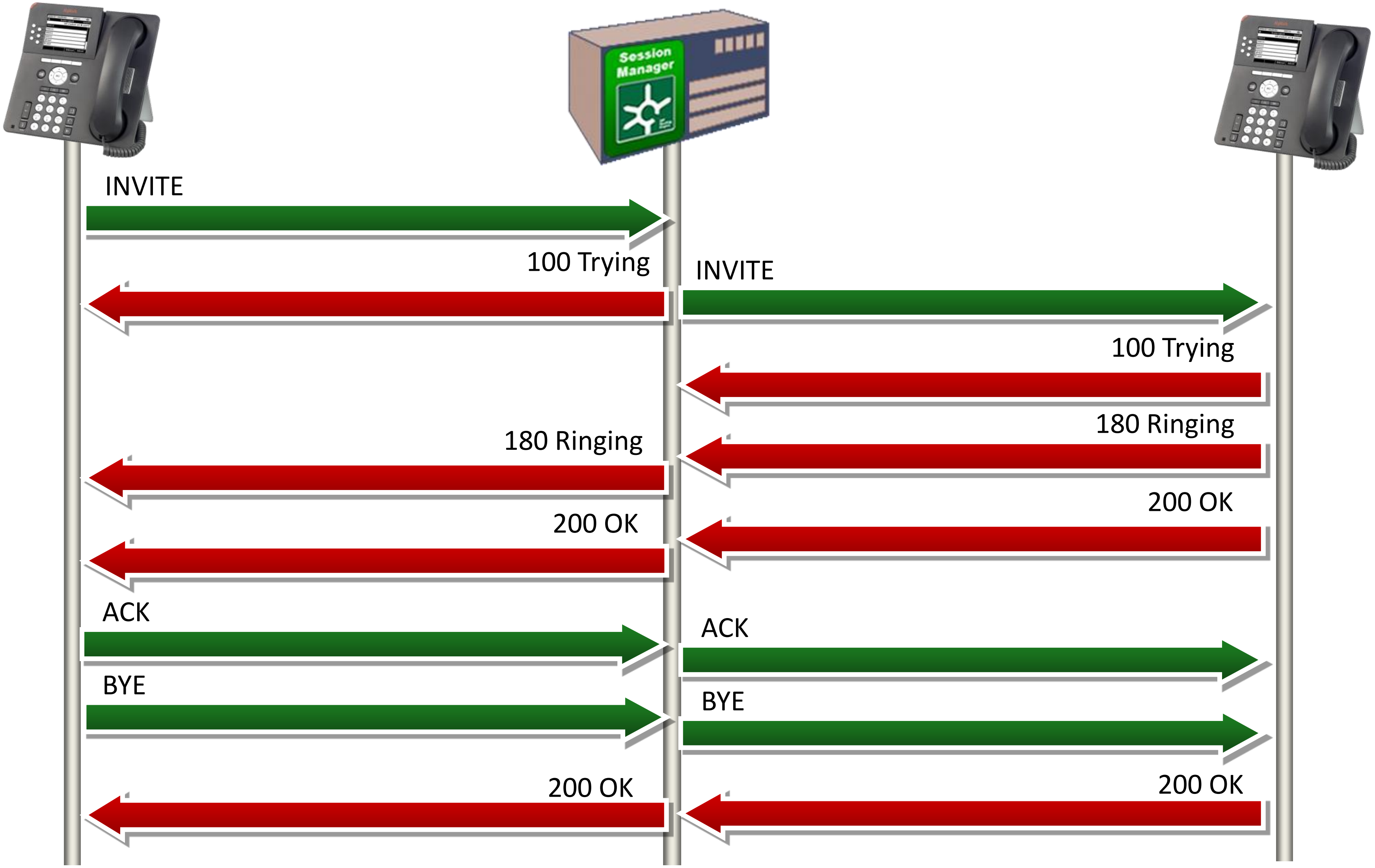
Yes!

No.

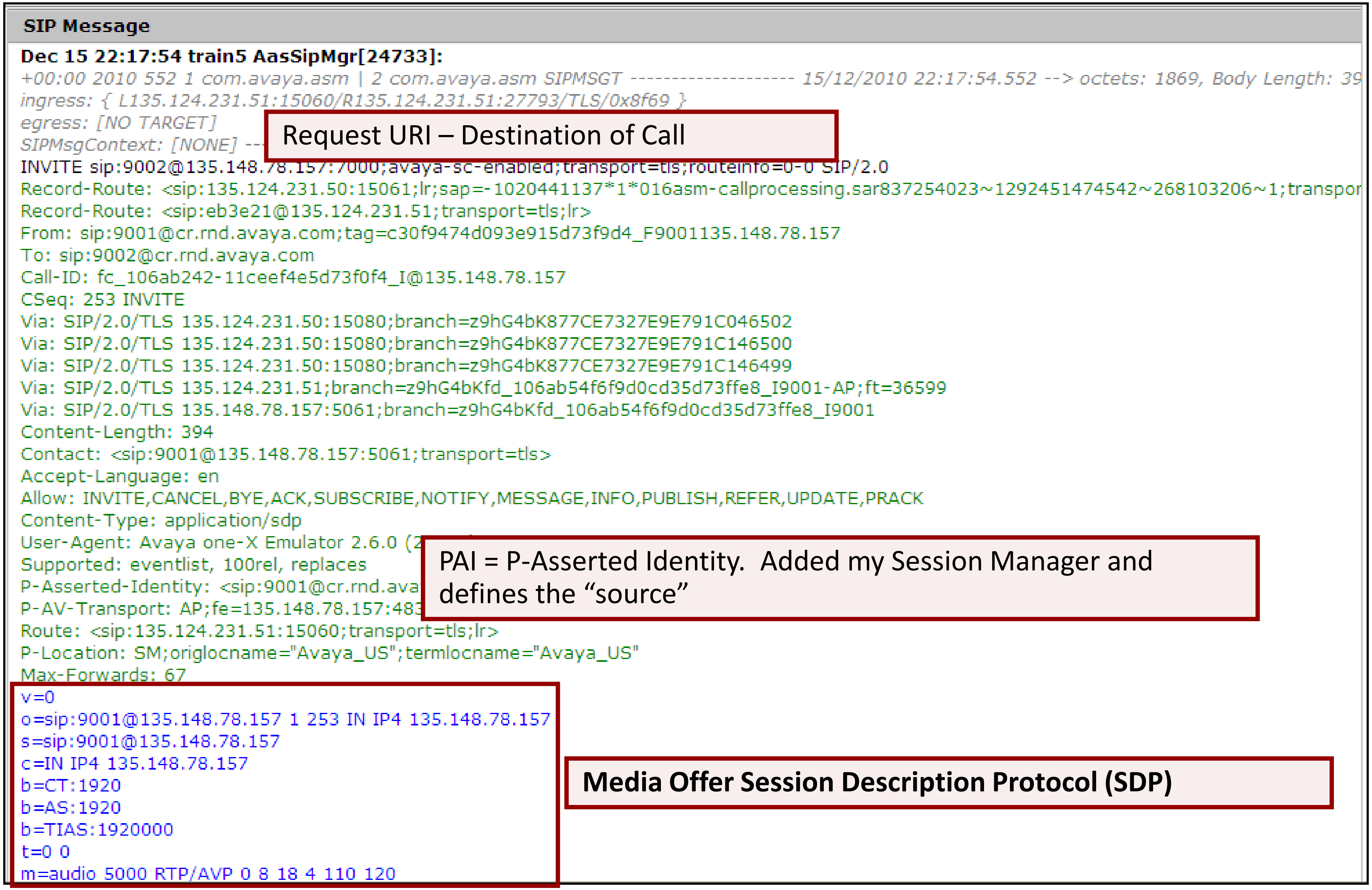
If not, do the following:

1. Retrace and validate your configuration
2. Run traceSM to diagnose the call flow and search for errors

Sample Successful INVITE Trace



Sample INVITE- SIP Primer



SIP Message

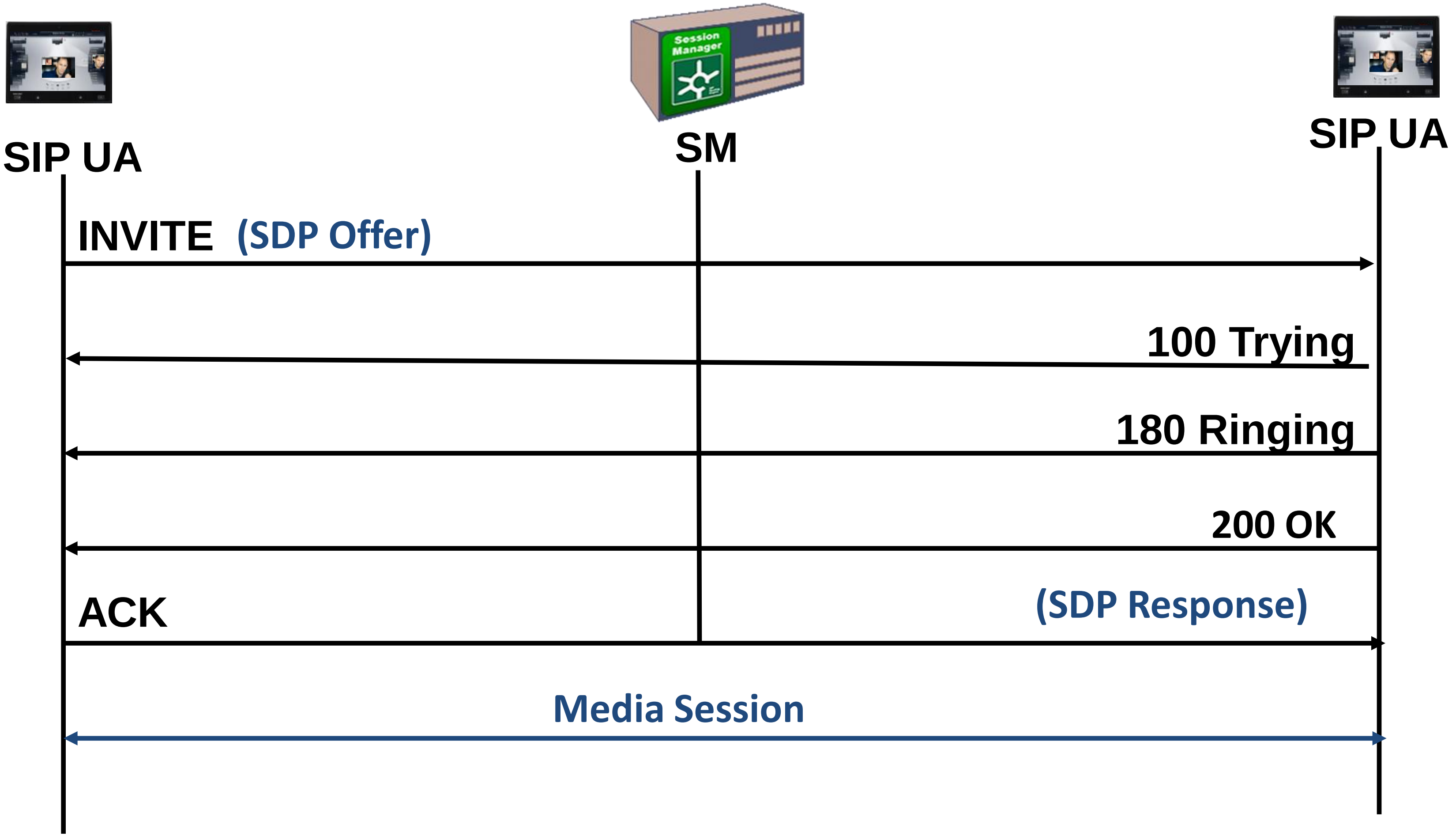
```
Dec 15 22:17:54 train5 AasSipMgr[24733]:
+00:00 2010 552 1 com.avaya.asm | 2 com.avaya.asm SIPMSGT -------------------- 15/12/2010 22:17:54.552 --> octets: 1869, Body Length: 39
ingress: { L135.124.231.51:15060/R135.124.231.51:27793/TLS/0x8f69 }
egress: [NO TARGET]
SIPMsgContext: [NONE] --
INVITE sip:9002@135.148.78.157:7000;avaya-sc-enabled;transport=tls;routeinfo=0-0 SIP/2.0
Record-Route: <sip:135.124.231.50:15061;lr;sap=-1020441137*1*016asm-callprocessing.sar837254023~1292451474542~268103206~1;transpor
Record-Route: <sip:eb3e21@135.124.231.51;transport=tls;lr>
From: sip:9001@cr.rnd.avaya.com;tag=c30f9474d093e915d73f9d4_F9001135.148.78.157
To: sip:9002@cr.rnd.avaya.com
Call-ID: fc_106ab242-11ceef4e5d73f0f4_I@135.148.78.157
CSeq: 253 INVITE
Via: SIP/2.0/TLS 135.124.231.50:15080;branch=z9hG4bK877CE7327E9E791C046502
Via: SIP/2.0/TLS 135.124.231.50:15080;branch=z9hG4bK877CE7327E9E791C146500
Via: SIP/2.0/TLS 135.124.231.50:15080;branch=z9hG4bK877CE7327E9E791C146499
Via: SIP/2.0/TLS 135.124.231.51;branch=z9hG4bKfd_106ab54f6f9d0cd35d73ffe8_I9001-AP;ft=36599
Via: SIP/2.0/TLS 135.148.78.157:5061;branch=z9hG4bKfd_106ab54f6f9d0cd35d73ffe8_I9001
Content-Length: 394
Contact: <sip:9001@135.148.78.157:5061;transport=tls>
Accept-Language: en
Allow: INVITE,CANCEL,BYE,ACK,SUBSCRIBE,NOTIFY,MESSAGE,INFO,PUBLISH,REFER,UPDATE,PRACK
Content-Type: application/sdp
User-Agent: Avaya one-X Emulator 2.6.0 (2
Supported: eventlist, 100rel, replaces
P-Asserted-Identity: <sip:9001@cr.rnd.ava
P-AV-Transport: AP;fe=135.148.78.157:483
Route: <sip:135.124.231.51:15060;transport=tls;lr>
P-Location: SM;origlocname="Avaya_US";termlocname="Avaya_US"
Max-Forwards: 67
v=0
o=sip:9001@135.148.78.157 1 253 IN IP4 135.148.78.157
s=sip:9001@135.148.78.157
c=IN IP4 135.148.78.157
b=CT:1920
b=AS:1920
b=TIAS:1920000
t=0 0
m=audio 5000 RTP/AVP 0 8 18 4 110 120
```

Request URI – Destination of Call

PAI = P-Asserted Identity. Added my Session Manager and defines the “source”

Media Offer Session Description Protocol (SDP)

When do SDPs get exchanged?



An SDP Offer / Response, between one-X Communicator ↔ Avaya1030

Offer

```
v=0
o=sip:<ext>@<orig-host>1 11 IN IP4
<orig-host>
s=sip:<ext>@<orig-host>
c=IN IP4 <host>
b=TIAS:13952000
t=0 0
m=audio 2048 RTP/AVP 9 18 110
b=TIAS:64000
a=rtpmap:9 G722/8000/1
a=rtpmap:18 G729/8000/1
a=fmtp:18 annexb=no
a=rtpmap:110 G726-32/8000/1
m=video 2688 RTP/AVP 109 34
b=TIAS:13888000
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42801f
a=rtpmap:34 H263/90000
a=fmtp:34 CIF4=1; CIF=1; QCIF=1;
SQCIF=1
```

Response

```
v=0
o=- 1 2 IN IP4 <term-host>
s=-
c=IN IP4 <term-host>
b=AS:1024
t=0 0
m=audio 60640 RTP/AVP 9 120
a=rtpmap:9 G722/8000
a=rtpmap:120 telephone-event/8000
m=video 60642 RTP/AVP 109 34
b=TIAS:1024000
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-
id=42801f;...
a=rtpmap:34 H263/90000
a=fmtp:34 CIF4=1;CIF=1;QCIF=1
```

Some SDP session descriptors

Session description

v= (Protocol version)

o= (owner/creator and session identifier).

s= (session name)

c=* (connection information)

b=* (bandwidth information)

m= (media name and transport address)

a=* (media attribute lines)

(‘*’ means it is optional)

Audio Codec Identification

0=PCMU (G711Mu)

3=GSM

4=G723

8=PCMA (G711A)

9=G722

15= G728

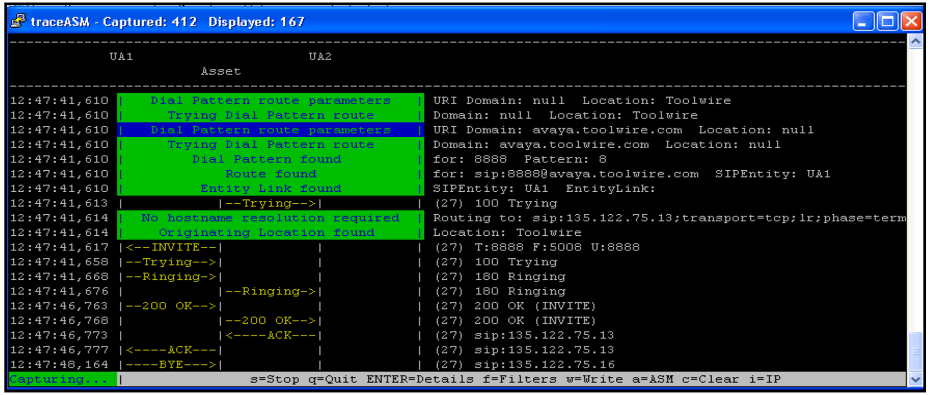
18= G729

Exercise: View Call Trace

Examine the trace and look for:

1. INVITE request
2. Req URI of caller and called party
3. The initial rejection of the INVITE and then the re-INVITE with the authentication details
4. 200 OK received by called party
5. Session Description where media and codecs are decided

Step	Action
1	Use the traceSM to view INVITE from **x9x1** to **X9x2**
2	View the results



```
traceASM - Captured: 412  Displayed: 167
------------------------------------------------------------------------------------------------------------------------
             UA1                        UA2
                        Asset
------------------------------------------------------------------------------------------------------------------------
12:47:41,610 |    Dial Pattern route parameters    | URI Domain: null  Location: Toolwire
12:47:41,610 |      Trying Dial Pattern route      | Domain: null  Location: Toolwire
12:47:41,610 |    Dial Pattern route parameters    | URI Domain: avaya.toolwire.com  Location: null
12:47:41,610 |      Trying Dial Pattern route      | Domain: avaya.toolwire.com  Location: null
12:47:41,610 |         Dial Pattern found          | for: 8888  Pattern: 8
12:47:41,610 |             Route found             | for: sip:8888@avaya.toolwire.com  SIPEntity: UA1
12:47:41,610 |          Entity Link found          | SIPEntity: UA1  EntityLink:
12:47:41,613 |           |--Trying-->|            | (27) 100 Trying
12:47:41,614 |   No hostname resolution required   | Routing to: sip:135.122.75.13;transport=tcp;lr;phase=term
12:47:41,614 |      Originating Location found     | Location: Toolwire
12:47:41,617 |<--INVITE--|            |            | (27) T:8888 F:5008 U:8888
12:47:41,658 |--Trying-->|            |            | (27) 100 Trying
12:47:41,668 |--Ringing->|            |            | (27) 180 Ringing
12:47:41,676 |           |--Ringing->|            | (27) 180 Ringing
12:47:46,763 |--200 OK-->|            |            | (27) 200 OK (INVITE)
12:47:46,768 |           |--200 OK-->|            | (27) 200 OK (INVITE)
12:47:46,773 |           |<----ACK---|            | (27) sip:135.122.75.13
12:47:46,777 |<----ACK---|            |            | (27) sip:135.122.75.13
12:47:48,164 |----BYE--->|            |            | (27) sip:135.122.75.16
Capturing... |        s=Stop q=Quit ENTER=Details f=Filters w=Write a=ASM c=Clear i=IP
```

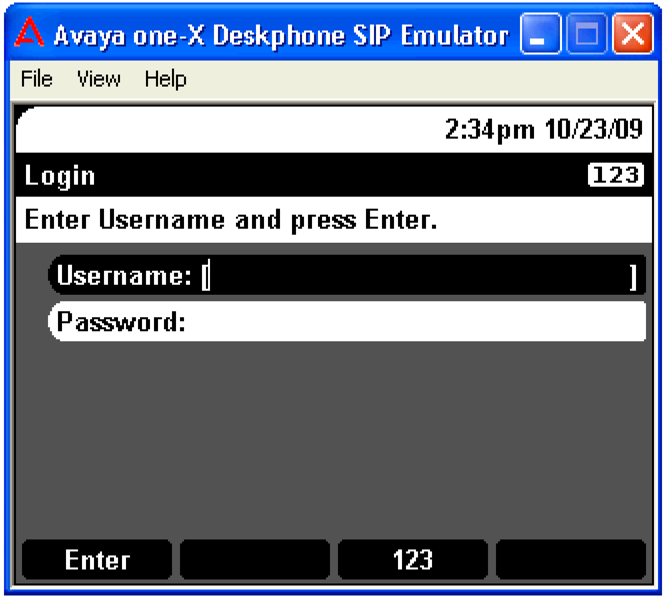
Note

Note

So we’ve got a call being routed entirely using SIP Registration & Registry Routing!

Exercise: Making a Call

Have x9x1 dial x9x4



Avaya one-X Deskphone SIP Emulator

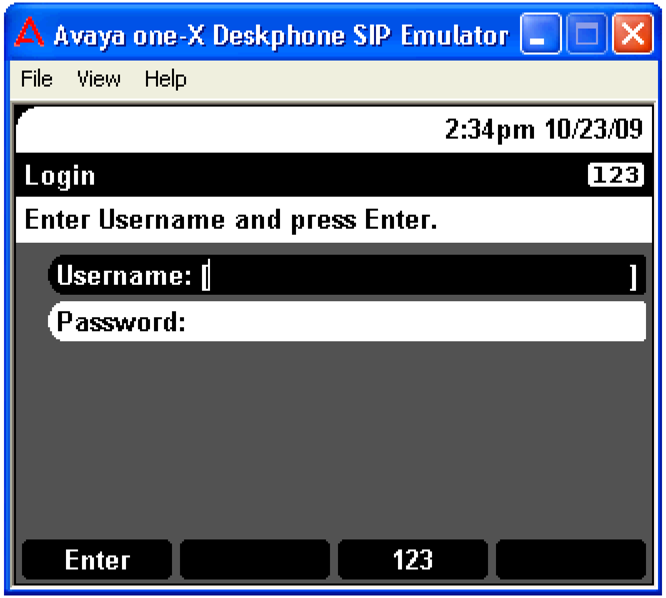
2:34pm 10/23/09

Login 123

Enter Username and press Enter.

Username: [ ]

Password:



Avaya one-X Deskphone SIP Emulator

2:34pm 10/23/09

Login 123

Enter Username and press Enter.

Username: [ ]

Password:

Did the call complete? Why not? Use the trace tool to help answer.

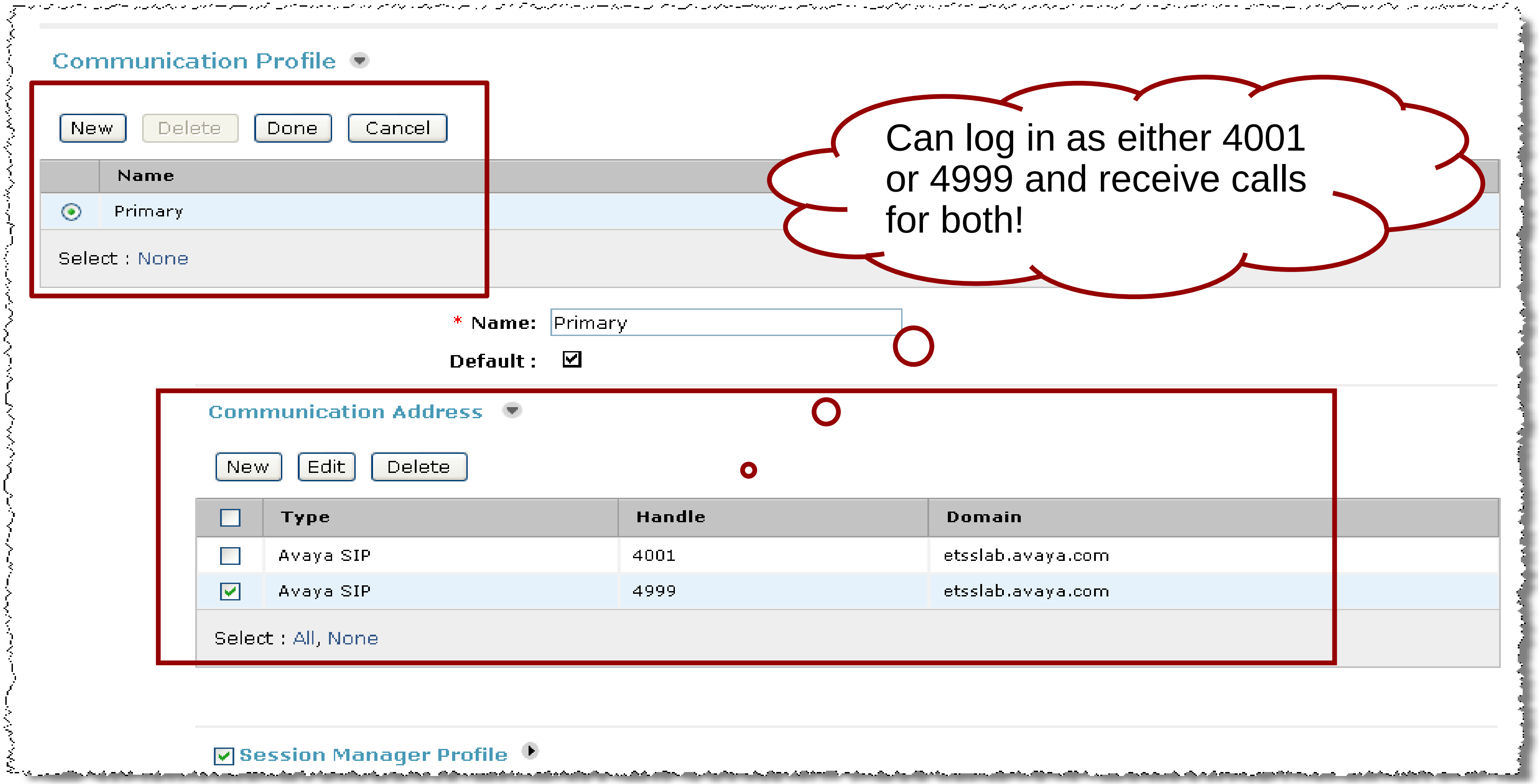
AVAYA | LEARNING

Multiple Addresses for a Single User

Communication Profile

Multiple Communication Addresses

- A single communication profile can have multiple communication addresses.



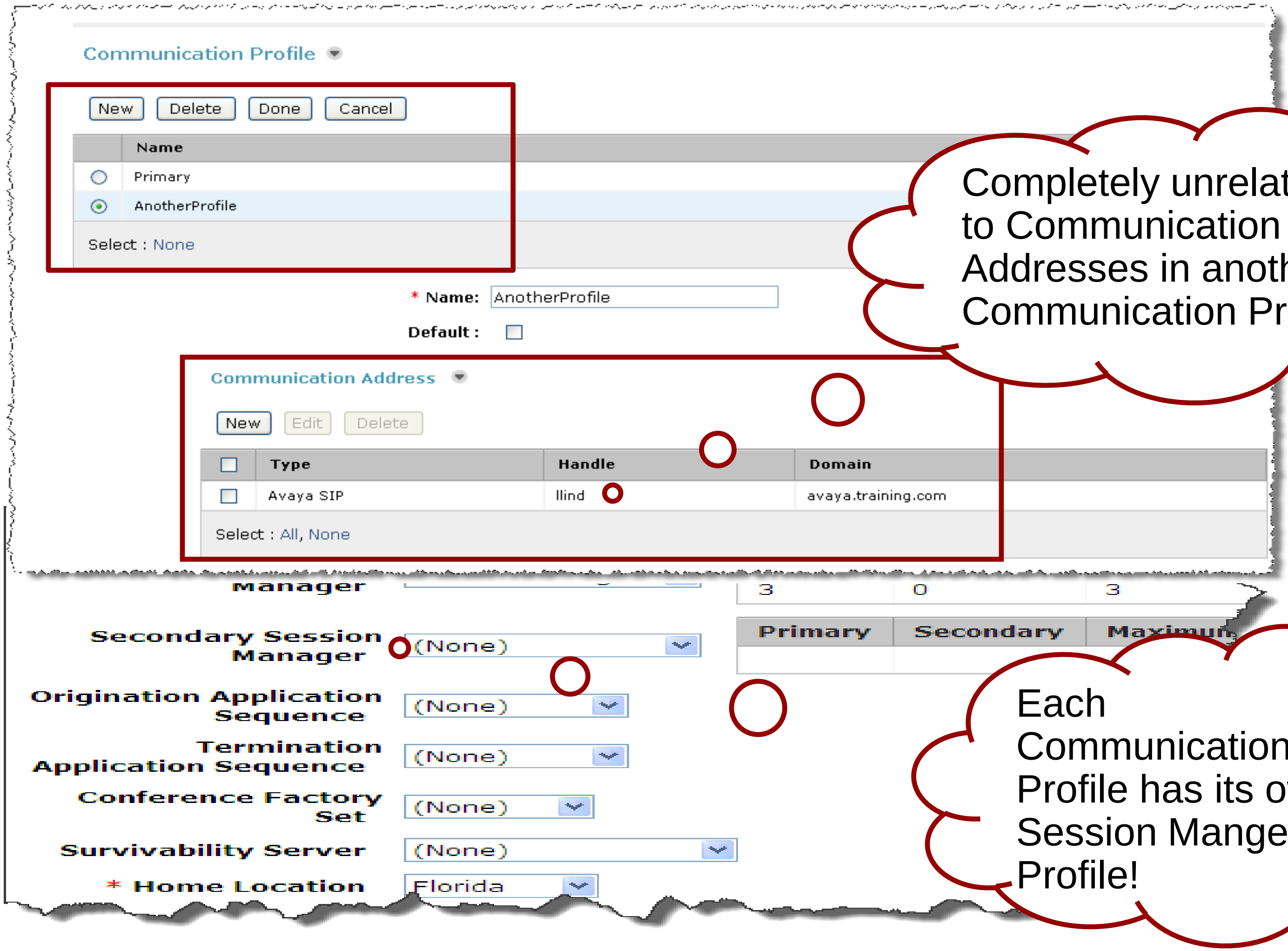
Can log in as either 4001 or 4999 and receive calls for both!

* Name: Primary

Default : ☑

□	Type	Handle	Domain
□	Avaya SIP	4001	etsslab.avaya.com
☑	Avaya SIP	4999	etsslab.avaya.com

Multiple Communication Profiles



Communication Profile

	Name
○	Primary
●	AnotherProfile

Select : None

* Name: AnotherProfile

Default : □

Communication Address

□	Type	Handle	Domain
□	Avaya SIP	llind	avaya.training.com

Select : All, None

3	0	3

Primary	Secondary	Maximum

Manager

Secondary Session Manager: (None)

Origination Application Sequence: (None)

Termination Application Sequence: (None)

Conference Factory Set: (None)

Survivability Server: (None)

* Home Location: Florida

Completely unrelated to Communication Addresses in another Communication Profile

Each Communication Profile has its own Session Manger Profile!

Lesson Summary

You have completed the following lesson objectives:

- Examine how Session Manager performs Registry Routing

Lesson 5

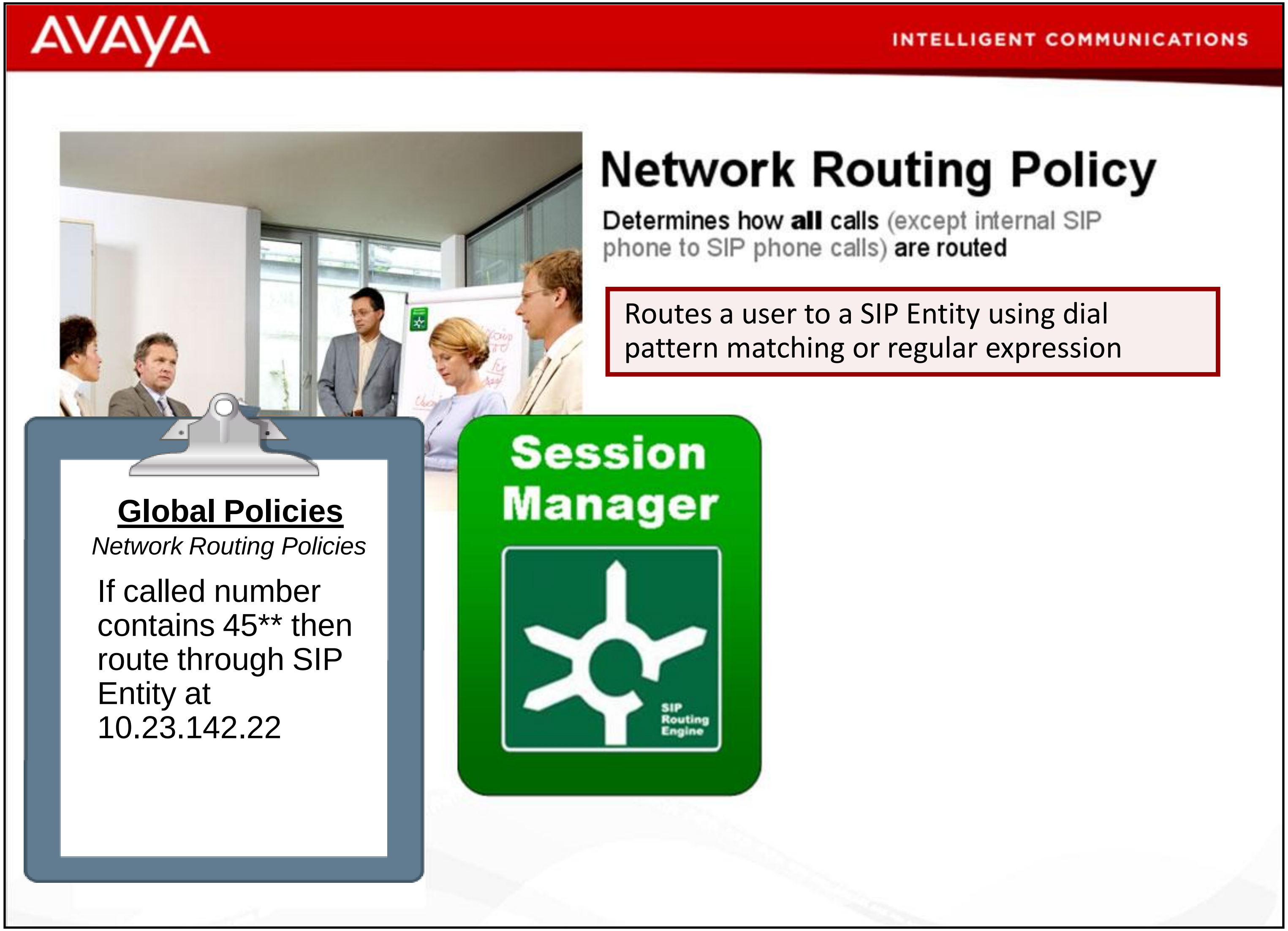
Centralized Routing II: NRP

Lesson Objectives

After completing this lesson, you will be able to:

- Review and configure the following to support centralized call routing within the enterprise:
  - Domain
  - Location
  - SIP Entities
  - Entity Links
  - Time Ranges
  - Routing Policies
  - Dial Patterns
  - Regular Expressions

Purpose of Session Manager Routing Policies



AVAYA
INTELLIGENT COMMUNICATIONS

Network Routing Policy

Determines how all calls (except internal SIP phone to SIP phone calls) **are routed**

Routes a user to a SIP Entity using dial pattern matching or regular expression

Global Policies

Network Routing Policies

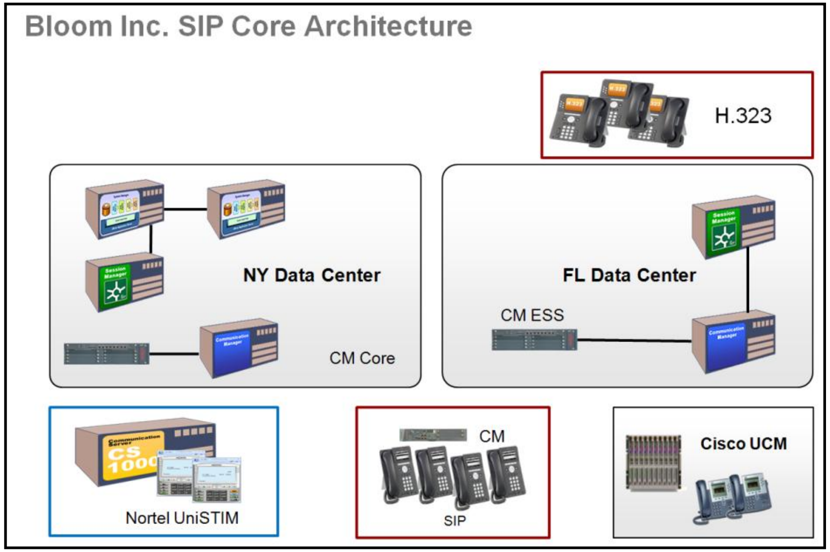
If called number contains 45** then route through SIP Entity at 10.23.142.22

Session Manager

SIP
Routing
Engine

Routing Design- What?

- What is/are the SIP domains?
- What SIP Entities exist?
- How many digits is it expecting?
- What are the extension ranges, DNIS digits expected by CM?
- What types of endpoints: H.323, SIP, Digital, Analog?



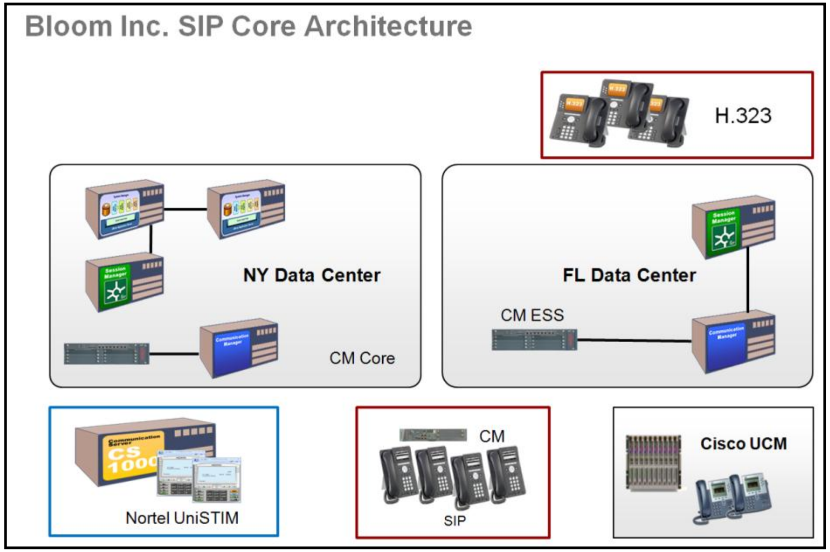
SIP Entities
Cisco UCM
Nortel CS1000
Communication Manager

Extensions (4-digit)
11xx to 69xx

Routing Design- When?

- What are the hours of operation?

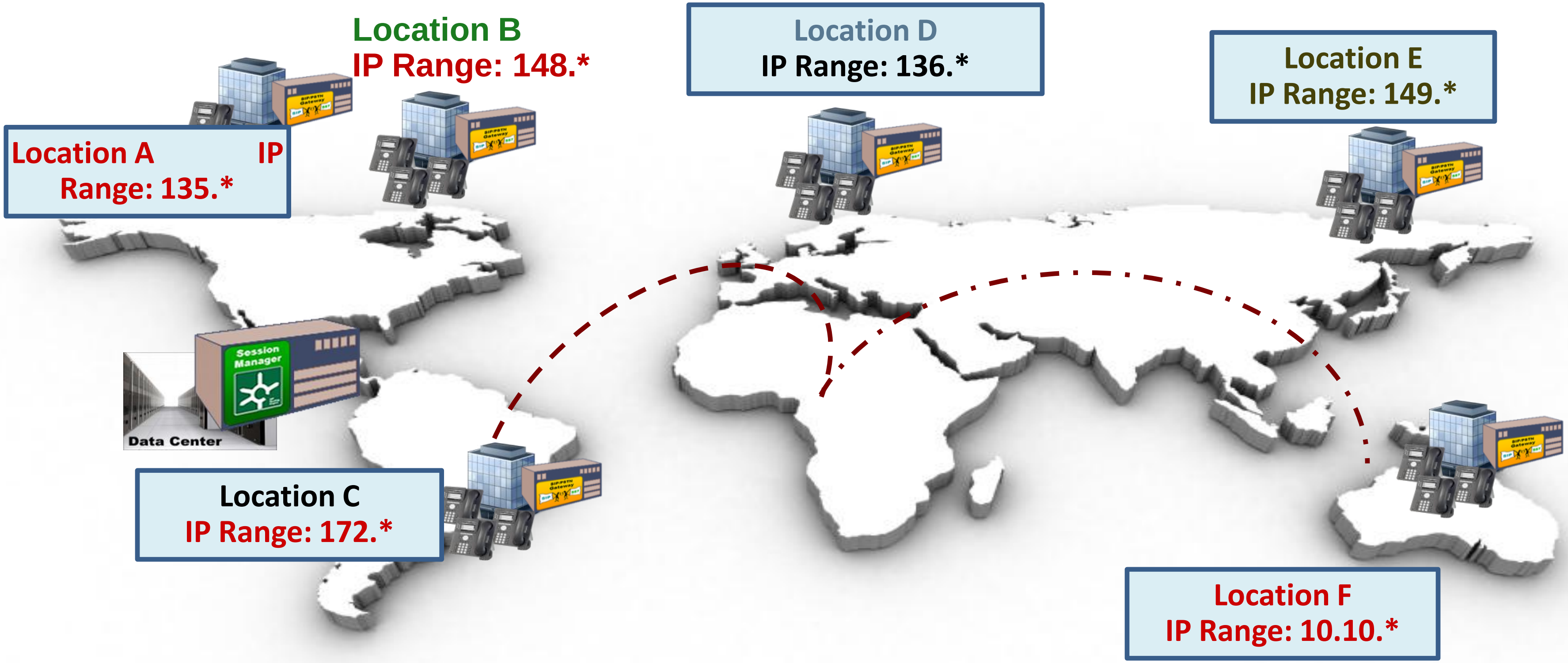
- “Thank you for calling Bloom Inc. Our hours of operation are
- Monday through Friday 7am to 7pm.”


Bloom Inc. SIP Core Architecture

Routing can be based on specific times of day and days of the week.

Routing Design- Where?

- Where is this SIP Entity located?
- How many locations are there?
- Can I use the network to route international calls and hop off to local trunks?



Location A IP Range: 135.*

Location B
IP Range: 148.*

Location C
IP Range: 172.*

Location D
IP Range: 136.*

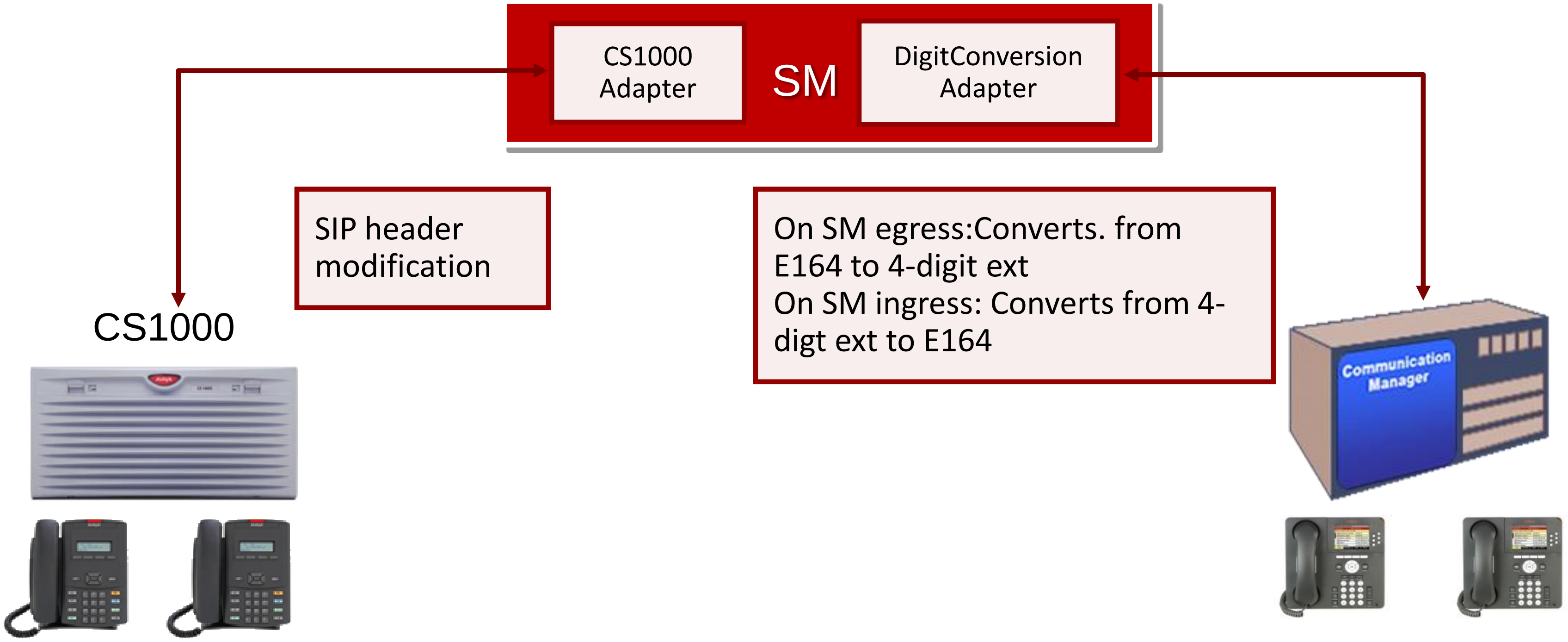
Location E
IP Range: 149.*

Location F
IP Range: 10.10.*

Tail-end Hop-off

Routing Design- How?

- Do I need to adapt the SIP request so it is understood by the receiving network or endpoint?
- What digits do I insert/delete to normalize my dial patterns in e164 format to Session Manager?
- Do I have to adapt the numbers CM receives/sends from/to Session Manager?
- Are there any 3rd Party SIP Entities that require special handling?



SIP header modification

On SM egress:Converts. from E164 to 4-digit ext
On SM ingress: Converts from 4-digt ext to E164

Creating Network Routing Policies

Lots to think about!

- These questions have to be answered and the appropriate records have to be added to the database in order to create routing policies.
- We’ll discuss those components in detail next.

Network Routing Policy

Determines how **all** calls (except internal SIP phone to SIP phone calls) are routed

Global Policies

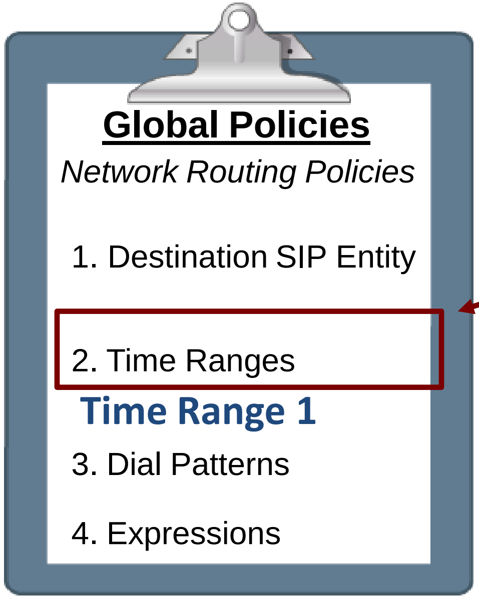
Network Routing Policies

If called number contains 45** then route through SIP Entity at 10.23.142.22

AVAYA
INTELLIGENT COMMUNICATIONS
Session Manager
SIP Routing Engine

Components of Routing Policies- Time Ranges

- Once I create my Time Ranges then I have a selection to choose from when creating my Routing Policies.



Global Policies

Network Routing Policies

1. Destination SIP Entity

2. Time Ranges

Time Range 1

3. Dial Patterns

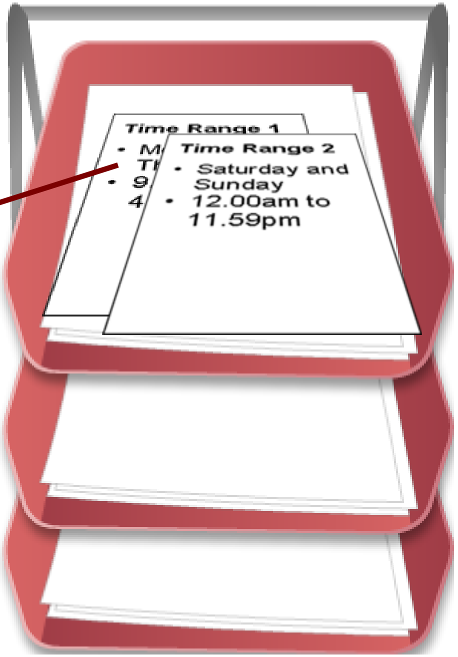
4. Expressions

Time Range 1

- Monday to Thursday
- 9.00am to 4.00pm

Time Range 2

- Saturday and Sunday
- 12.00am to 11.59pm



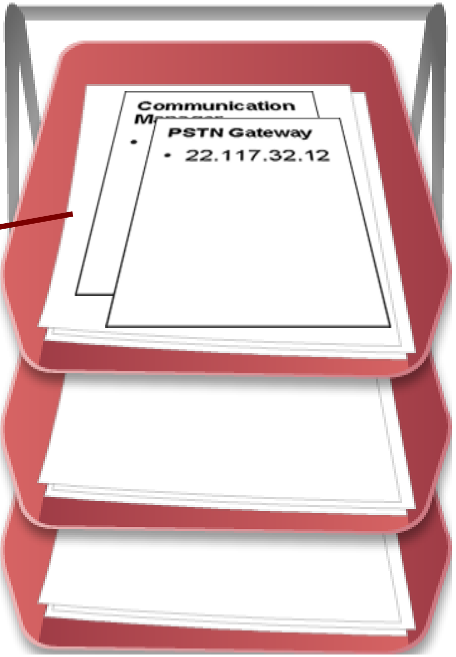
Time Ranges

Components of Routing Policies- SIP Entities

Global Policies

Network Routing Policies

1. Destination SIP Entity
   PSTN Gateway
2. Time Ranges
   Time Range 1
3. Dial Patterns
4. Expressions



Communication Manager

- 10.24.35.112

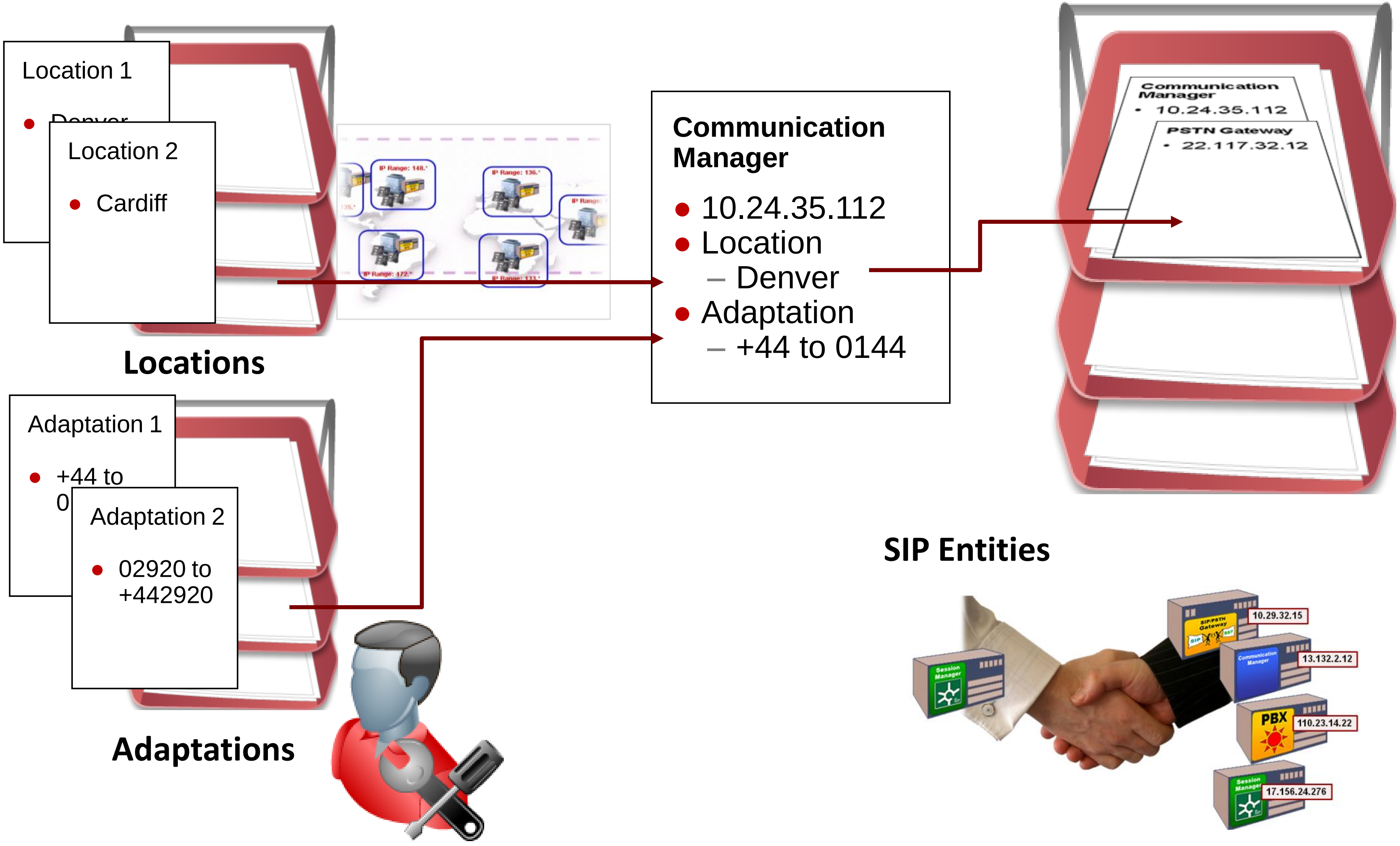
PSTN Gateway

- 22.117.32.12

SIP Entities

SIP/PSTN Gateway
SIP
SST
10.29.32.15
Communication Manager
13.132.2.12
PBX
110.23.14.22
Session Manager
Session Manager
17.156.24.276

Components of Routing Policies- Locations



Location 1

- Denver

Location 2

- Cardiff

Locations

Communication Manager

- 10.24.35.112
- Location
  - Denver
- Adaptation
  - +44 to 0144

Adaptation 1

- +44 to 0

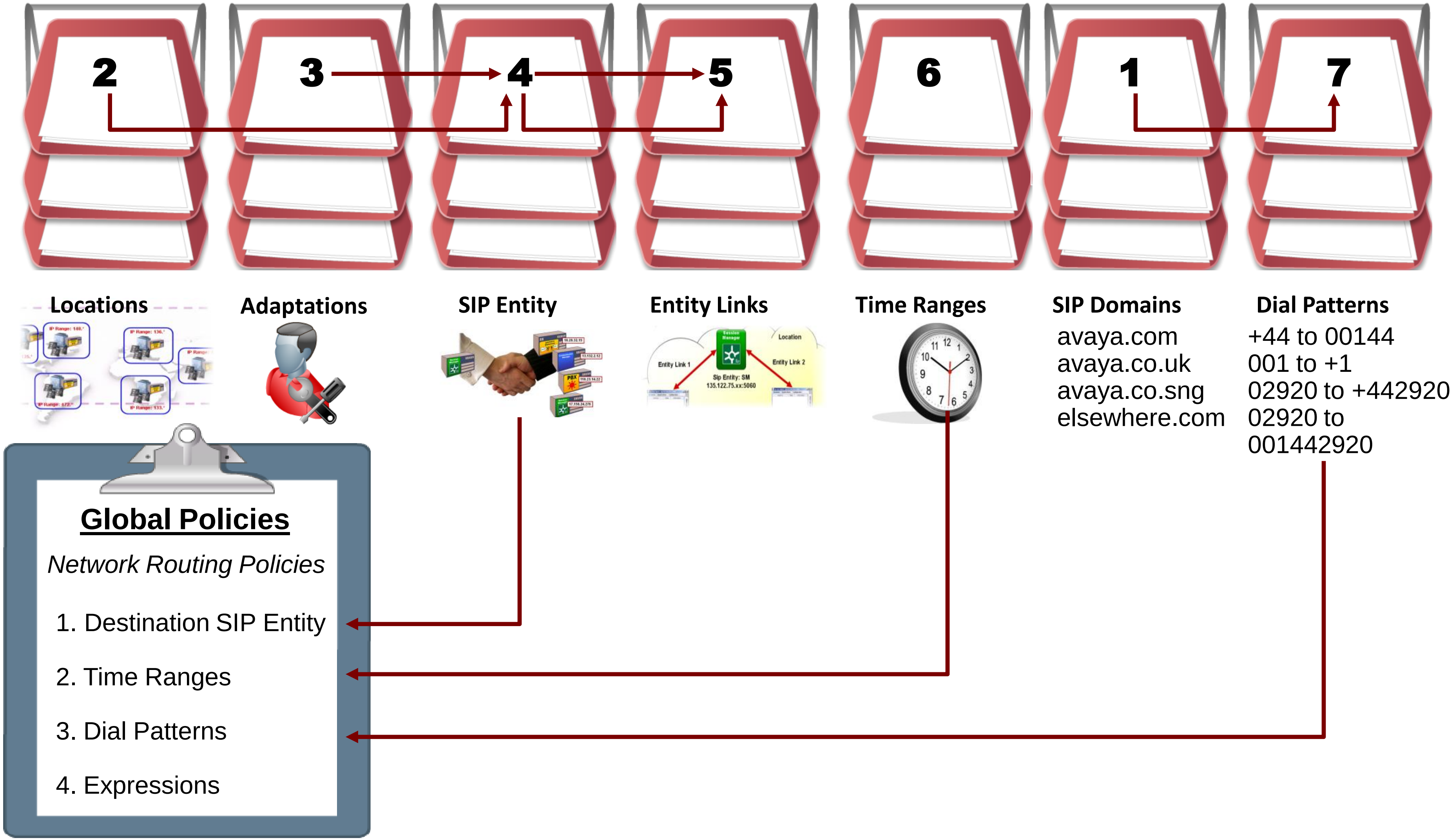
Adaptation 2

- 02920 to +442920

Adaptations

SIP Entities

Components of Routing Policies- Locations (continued)



Locations

Adaptations

SIP Entity

Entity Links

Time Ranges

SIP Domains

avaya.com
avaya.co.uk
avaya.co.sng
elsewhere.com

Dial Patterns

+44 to 00144
001 to +1
02920 to +442920
02920 to 001442920

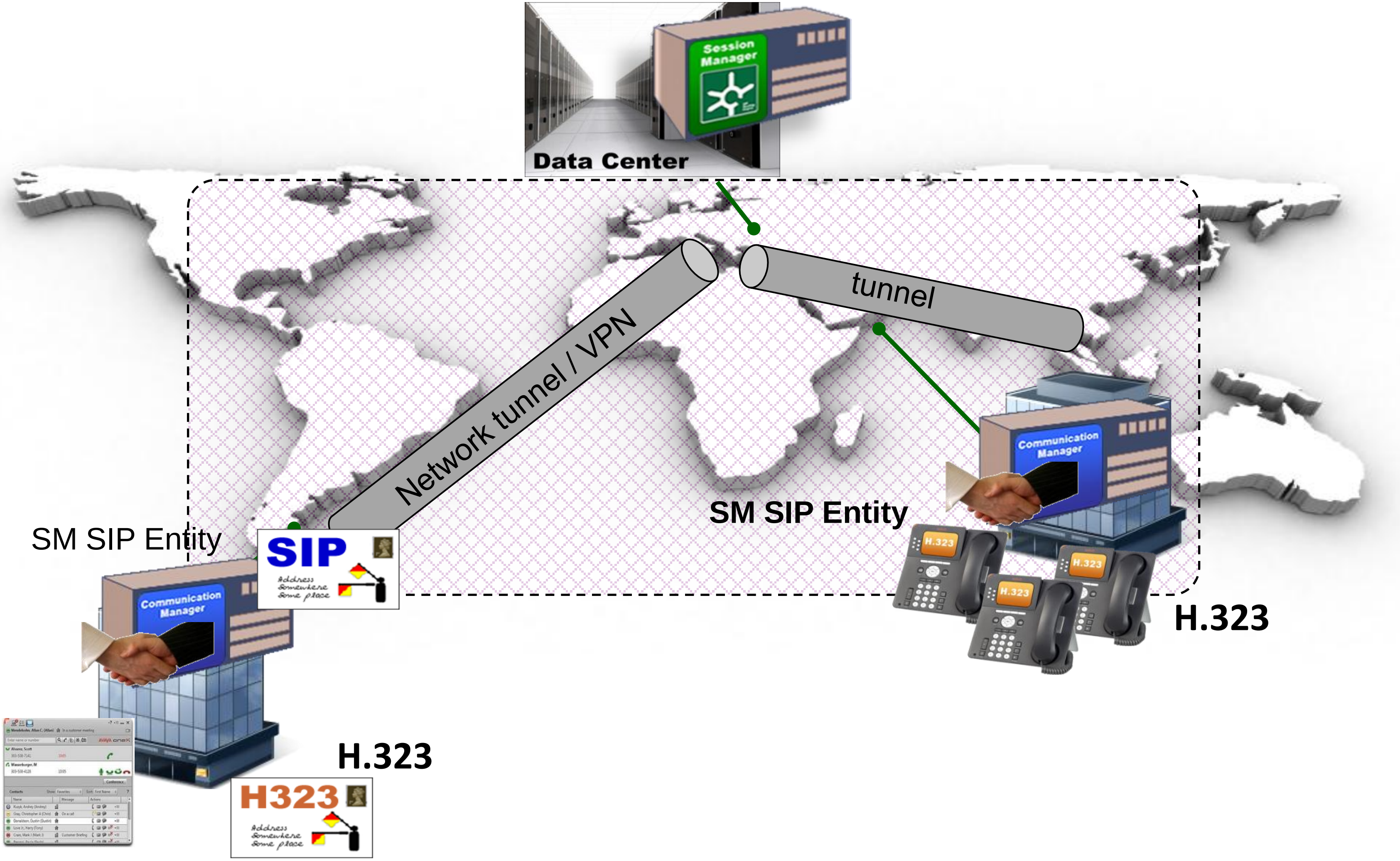
Global Policies

Network Routing Policies

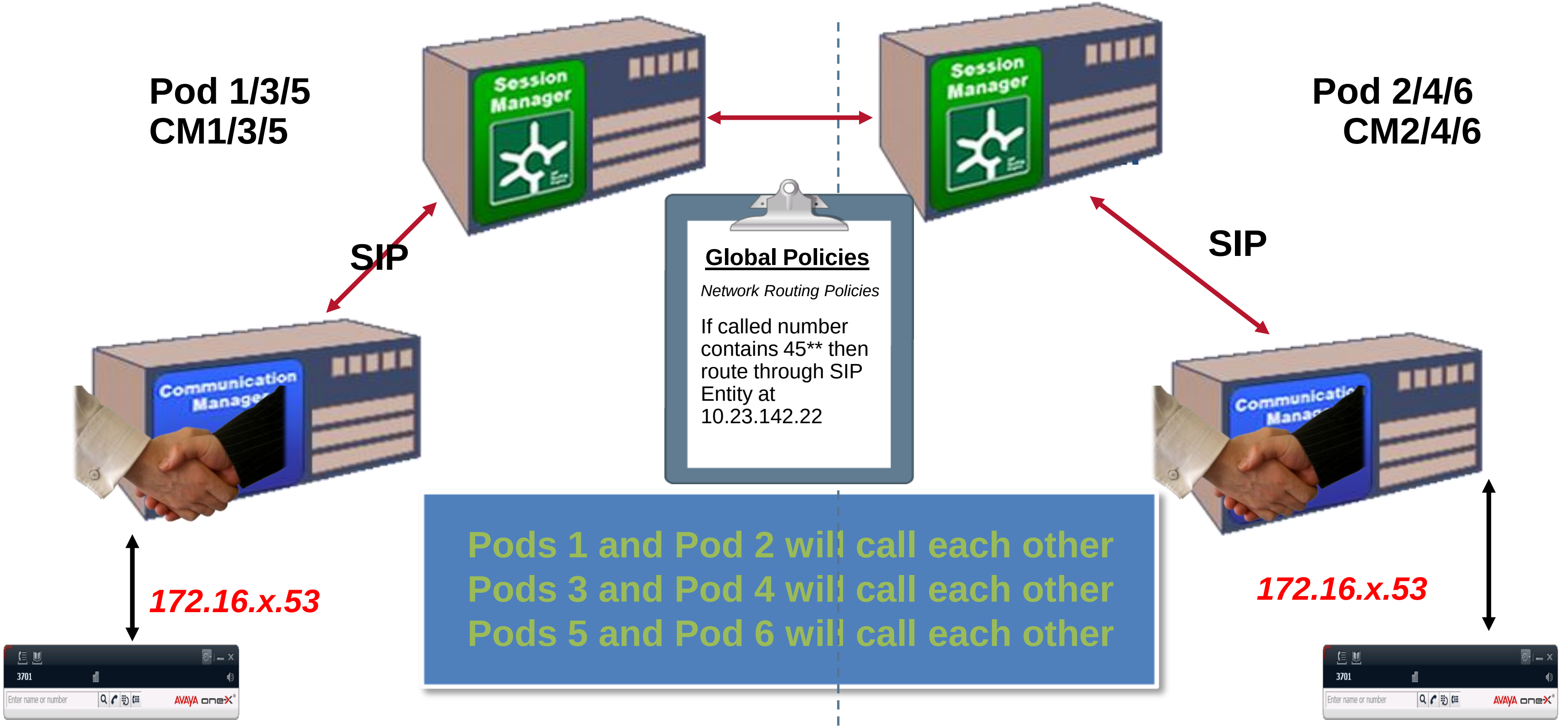
1. Destination SIP Entity
2. Time Ranges
3. Dial Patterns
4. Expressions

Defining the SIP Routing Policy

Session Manager & Communication Manager



Routing Scenario 1:
H.323 to H.323 Call Routing through Session Manager



Global Policies

Network Routing Policies

If called number contains 45** then route through SIP Entity at 10.23.142.22

Pods 1 and Pod 2 will call each other
Pods 3 and Pod 4 will call each other
Pods 5 and Pod 6 will call each other

H.323

H.323

Student	Pod 1	Pod 2	Pod 3	Pod 4	Pod 5	Pod 6
Student a	1711	2711	3711	4711	5711	6711
Student b	1721	2721	3721	4721	5721	6721

AVAYA | LEARNING

SIP Domains Review

Components of Routing Policies- SIP Domains

Locations

Adaptations

SIP Entity

Entity Links

Time Ranges

SIP Domains

avaya.com
avaya.co.uk
avaya.co.sng
elsewhere.com

Dial Patterns

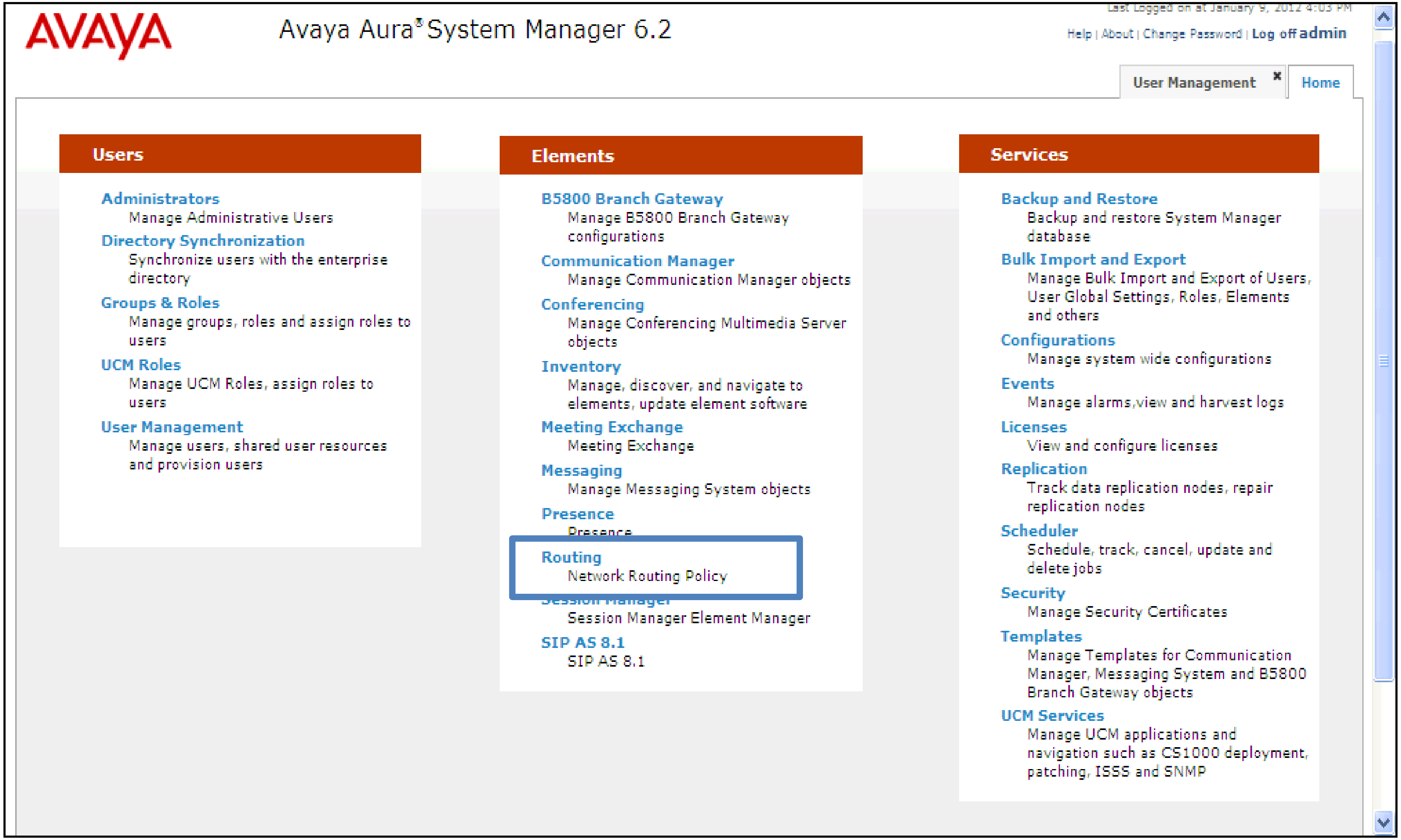
+44 to 00144
001 to +1
02920 to +442920
02920 to 001442920

Global Policies

Network Routing Policies

1. Destination SIP Entity
2. Time Ranges
3. Dial Patterns
4. Expressions

SIP Domains



Last Logged on at January 9, 2012 4:03 PM

Avaya Aura® System Manager 6.2

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

UCM Roles
Manage UCM Roles, assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway configurations

Communication Manager
Manage Communication Manager objects

Conferencing
Manage Conferencing Multimedia Server objects

Inventory
Manage, discover, and navigate to elements, update element software

Meeting Exchange
Meeting Exchange

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

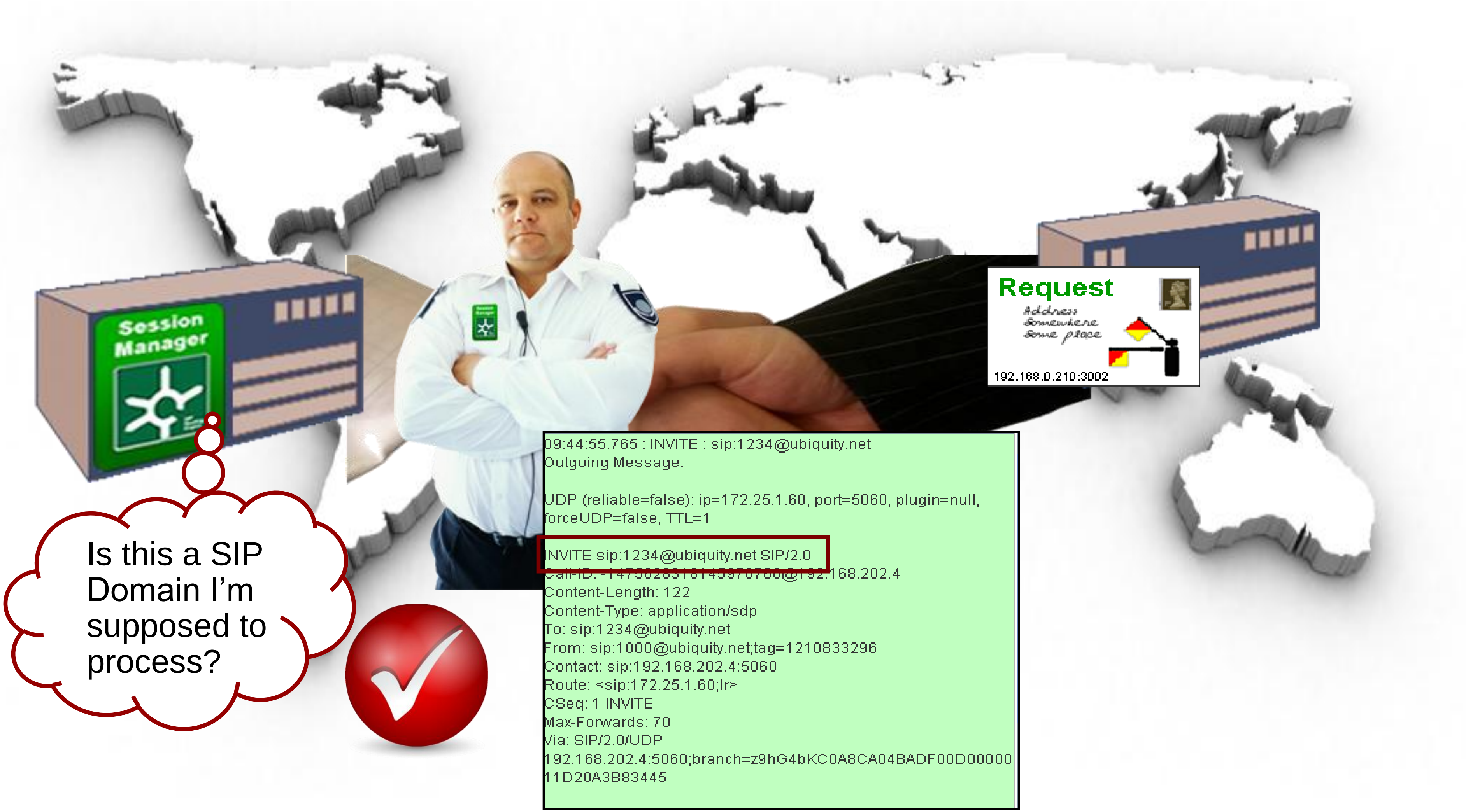
Scheduler
Schedule, track, cancel, update and delete jobs

Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway objects

UCM Services
Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

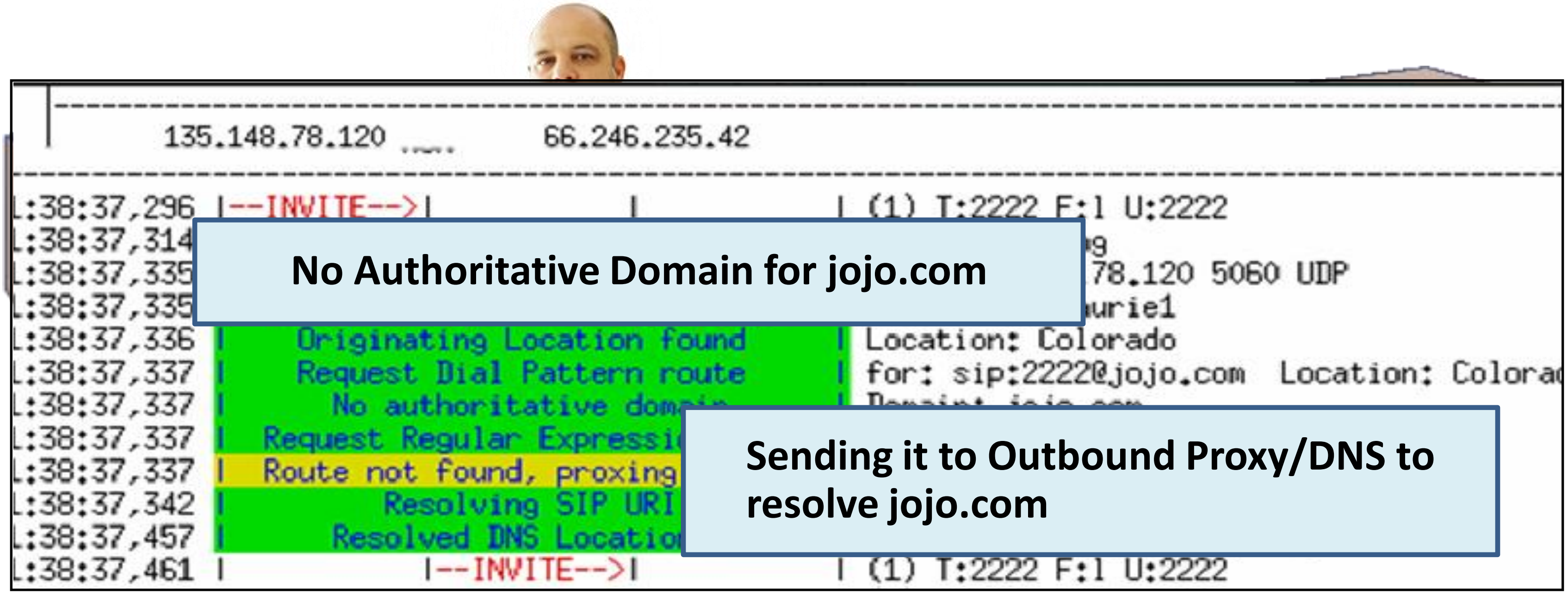
SIP Domains (continued)



```
09:44:55.765 : INVITE : sip:1234@ubiquity.net
Outgoing Message.

UDP (reliable=false): ip=172.25.1.60, port=5060, plugin=null,
forceUDP=false, TTL=1

INVITE sip:1234@ubiquity.net SIP/2.0
Call-ID: -1475028518145970760@192.168.202.4
Content-Length: 122
Content-Type: application/sdp
To: sip:1234@ubiquity.net
From: sip:1000@ubiquity.net;tag=1210833296
Contact: sip:192.168.202.4:5060
Route: <sip:172.25.1.60;lr>
CSeq: 1 INVITE
Max-Forwards: 70
Via: SIP/2.0/UDP
192.168.202.4:5060;branch=z9hG4bKC0A8CA04BADF00D00000
11D20A3B83445
```

SIP Domains – No Authoritative Domain

1. Every SIP domain must be configured in order for Session Manager to route to it.
2. If it receives a request from a domain for which it is not authoritative then it will send it to DNS to resolve.



```
|------------------------------------------------------------------------------------------
|       135.148.78.120 ....       66.246.235.42
-------------------------------------------------------------------------------------------
L:38:37,296 |--INVITE-->|          |           | (1) T:2222 F:1 U:2222
L:38:37,314                                                   g
L:38:37,335                                               78.120 5060 UDP
L:38:37,335                                               urie1
L:38:37,336 |    Originating Location found    | Location: Colorado
L:38:37,337 |    Request Dial Pattern route    | for: sip:2222@jojo.com  Location: Colora
L:38:37,337 |      No authoritative doma
L:38:37,337 |  Request Regular Expressi
L:38:37,337 |  Route not found, proxing
L:38:37,342 |          Resolving SIP URI
L:38:37,457 |       Resolved DNS Locatio
L:38:37,461 |          |--INVITE-->|         | (1) T:2222 F:1 U:2222
```

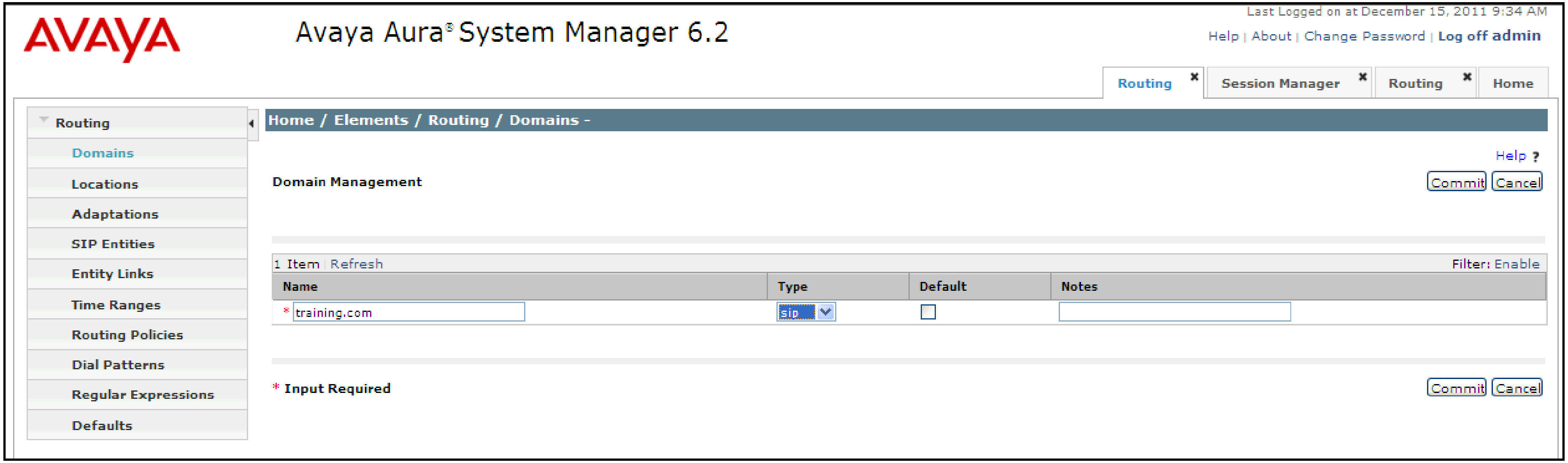
No Authoritative Domain for jojo.com

Sending it to Outbound Proxy/DNS to resolve jojo.com

SIP Domains

Only Domains of type **SIP** can be used for routing

Routing >> Domains



Domain Management

Name	Type	Default	Notes
* training.com	sip	□	

* Input Required

AVAYA | LEARNING

Locations Review

Components of Routing Policies- Locations

Locations

Adaptations

SIP Entity

Entity Links

Session Manager
Location
Entity Link 1
Entity Link 2
Sip Entity: SM
135.122.75.xx:5060

Time Ranges

SIP Domains

avaya.com
avaya.co.uk
avaya.co.sng
elsewhere.com

Dial Patterns

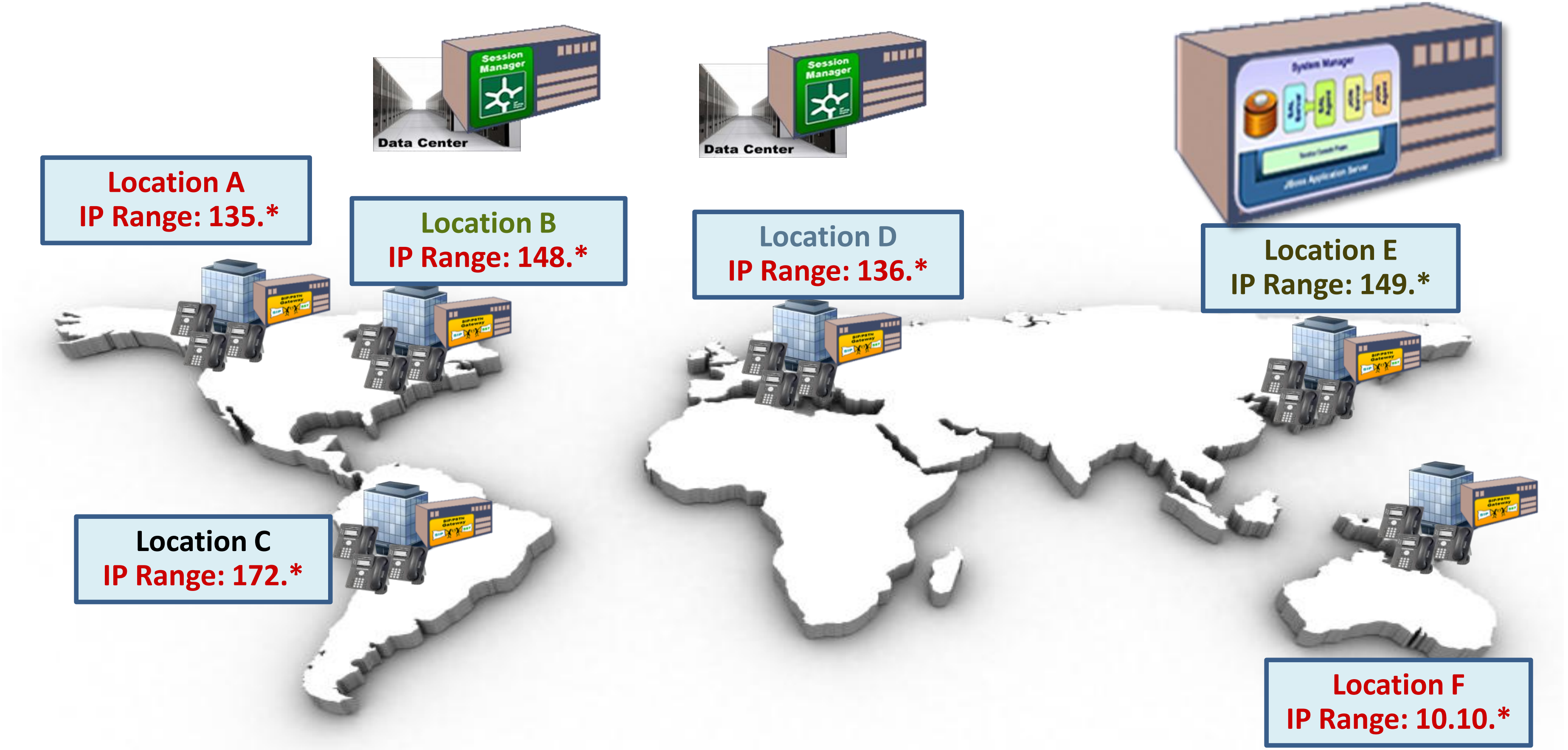
+44 to 00144
001 to +1
02920 to +442920
02920 to 001442920

Global Policies

Network Routing Policies

1. Destination SIP Entity
2. Time Ranges
3. Dial Patterns
4. Expressions

Network Locations



Location A
IP Range: 135.*

Location B
IP Range: 148.*

Location D
IP Range: 136.*

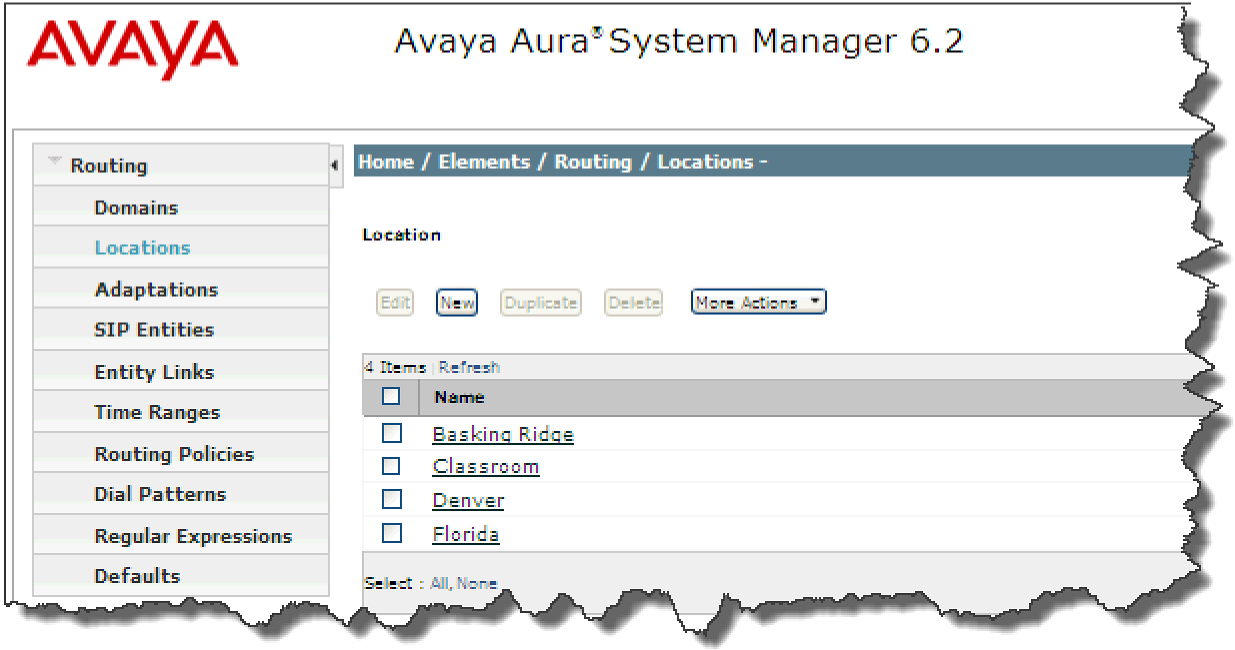
Location E
IP Range: 149.*

Location C
IP Range: 172.*

Location F
IP Range: 10.10.*

Locations

Routing >> Locations

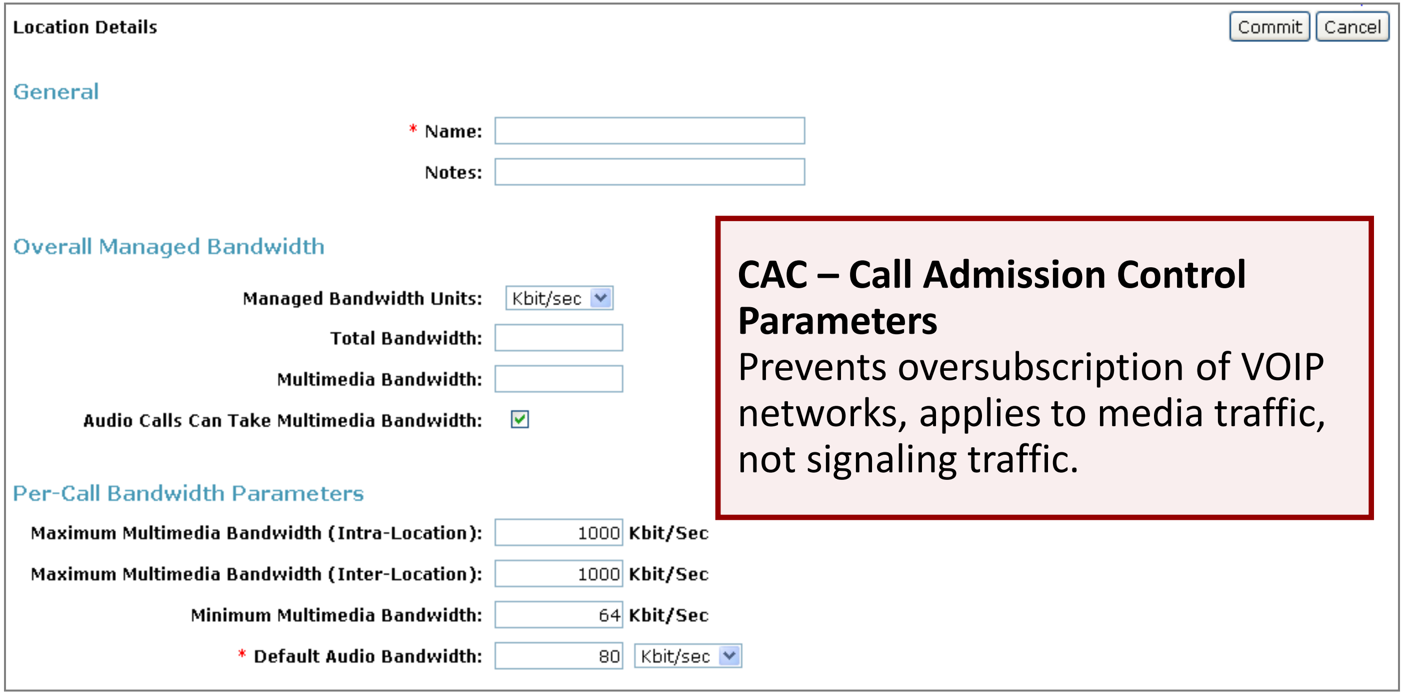


□	Name
□	Basking Ridge
□	Classroom
□	Denver
□	Florida

The Location associates an IP address pattern with a name to be used in the Routing Policy to determine the originating location of a call. Locations also set the Call Admission Control parameters.

Locations (continued)

- Session Manager can manage bandwidth parameters to each location from this screen.
- It is activated once you enter a value in the Total Bandwidth field



Location Details

General

* Name:	
Notes:	

Overall Managed Bandwidth

Managed Bandwidth Units:	Kbit/sec
Total Bandwidth:	
Multimedia Bandwidth:	
Audio Calls Can Take Multimedia Bandwidth:	☑

Per-Call Bandwidth Parameters

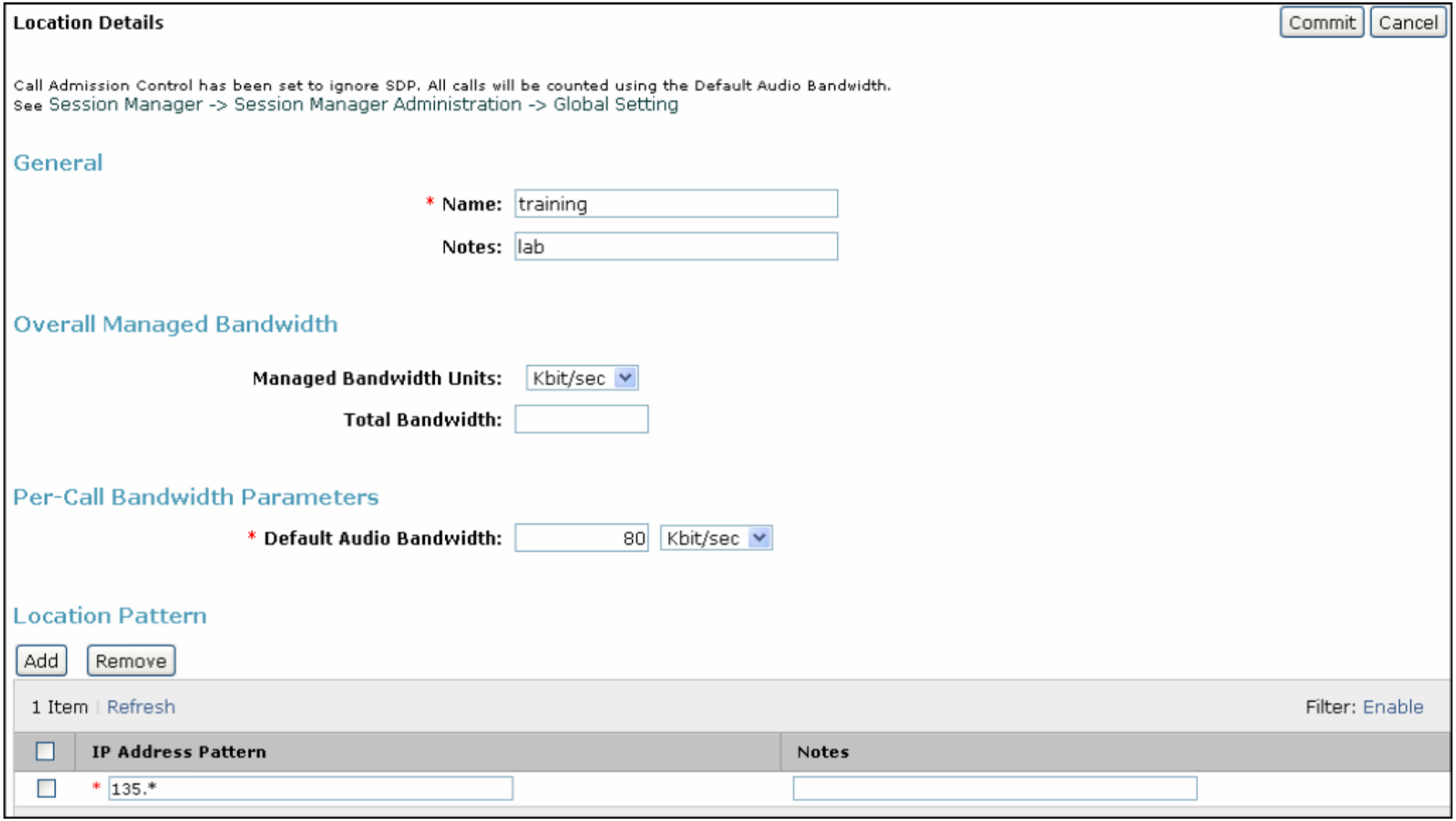
Maximum Multimedia Bandwidth (Intra-Location):	1000 Kbit/Sec
Maximum Multimedia Bandwidth (Inter-Location):	1000 Kbit/Sec
Minimum Multimedia Bandwidth:	64 Kbit/Sec
* Default Audio Bandwidth:	80 Kbit/sec

CAC – Call Admission Control Parameters
Prevents oversubscription of VOIP networks, applies to media traffic, not signaling traffic.

- You can segment the bandwidth between audio and video traffic on the network.
- Each Location has a "bandwidth per call" and a "total managed bandwidth"

Locations are already configured

Routing >> Locations



Location Details

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See Session Manager -> Session Manager Administration -> Global Setting

General

* Name:	training
Notes:	lab

Overall Managed Bandwidth

Managed Bandwidth Units:	Kbit/sec
Total Bandwidth:	

Per-Call Bandwidth Parameters

* Default Audio Bandwidth:	80	Kbit/sec

Location Pattern

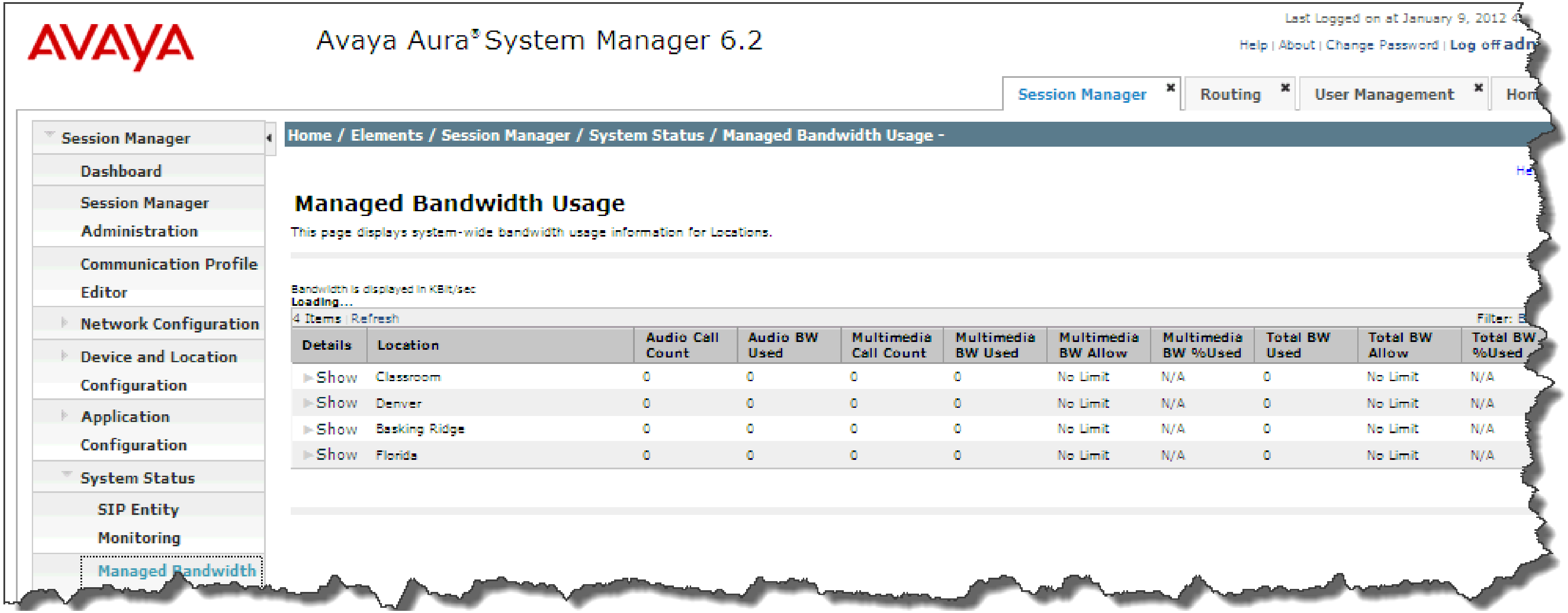
1 Item | Refresh

Filter: Enable

□	IP Address Pattern	Notes
□	* 135.*	

Managed Bandwidth Usage

- Displays system-wide bandwidth usage information for locations where usage is managed.
- The details expansion shows the breakdown of usage among Session Manager Instances.



AVAYA
Avaya Aura® System Manager 6.2
Last Logged on at January 9, 2012 4
Help | About | Change Password | Log off adn
Session Manager
Routing
User Management
Hon
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
SIP Entity Monitoring
Managed Bandwidth
Home / Elements / Session Manager / System Status / Managed Bandwidth Usage -
He

Managed Bandwidth Usage

This page displays system-wide bandwidth usage information for Locations.

Bandwidth is displayed in KBit/sec

Loading...

4 Items | Refresh

Filter: E

Details	Location	Audio Call Count	Audio BW Used	Multimedia Call Count	Multimedia BW Used	Multimedia BW Allow	Multimedia BW %Used	Total BW Used	Total BW Allow	Total BW %Used
▶ Show	Classroom	0	0	0	0	No Limit	N/A	0	No Limit	N/A
▶ Show	Denver	0	0	0	0	No Limit	N/A	0	No Limit	N/A
▶ Show	Basking Ridge	0	0	0	0	No Limit	N/A	0	No Limit	N/A
▶ Show	Florida	0	0	0	0	No Limit	N/A	0	No Limit	N/A

Adaptations Review

Components of Routing Policies- Adaptations

Locations

Adaptations

SIP Entity

Entity Links

Time Ranges

SIP Domains

avaya.com
avaya.co.uk
avaya.co.sng
elsewhere.com

Dial Patterns

+44 to 00144
001 to +1
02920 to +442920
02920 to 001442920

Global Policies

Network Routing Policies

1. Destination SIP Entity
2. Time Ranges
3. Dial Patterns
4. Expressions

Not Required for this scenario.
More on these later!

AVAYA | LEARNING

SIP Entities

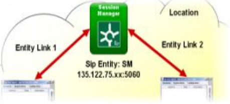
Components of Routing Policies- SIP Entities

Locations

Adaptations

SIP Entity

Entity Links



Time Ranges

SIP Domains

avaya.com
avaya.co.uk
avaya.co.sng
elsewhere.com

Dial Patterns

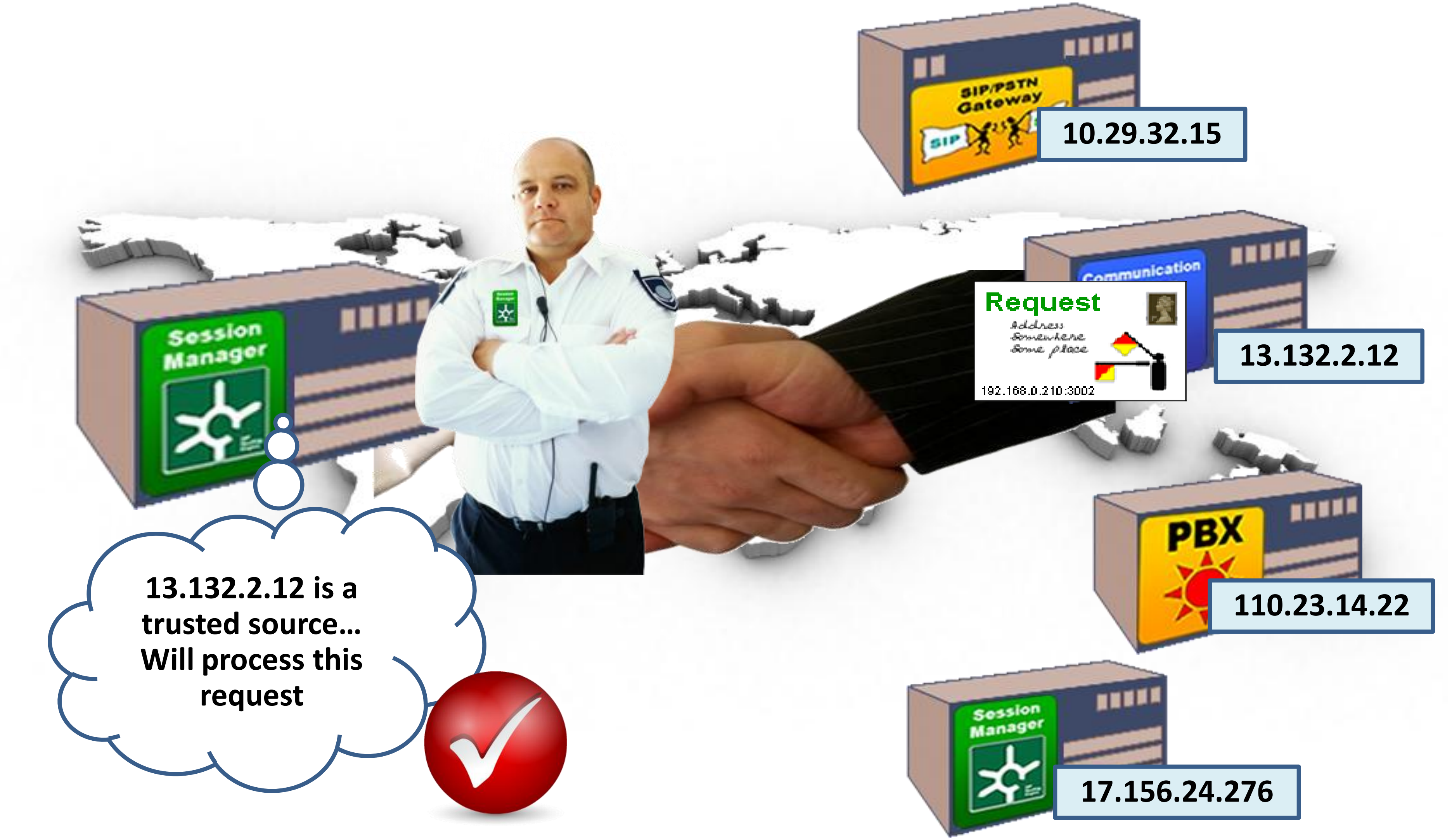
+44 to 00144
001 to +1
02920 to +442920
02920 to 001442920

Global Policies

Network Routing Policies

1. Destination SIP Entity
2. Time Ranges
3. Dial Patterns
4. Expressions

SIP Entities



10.29.32.15

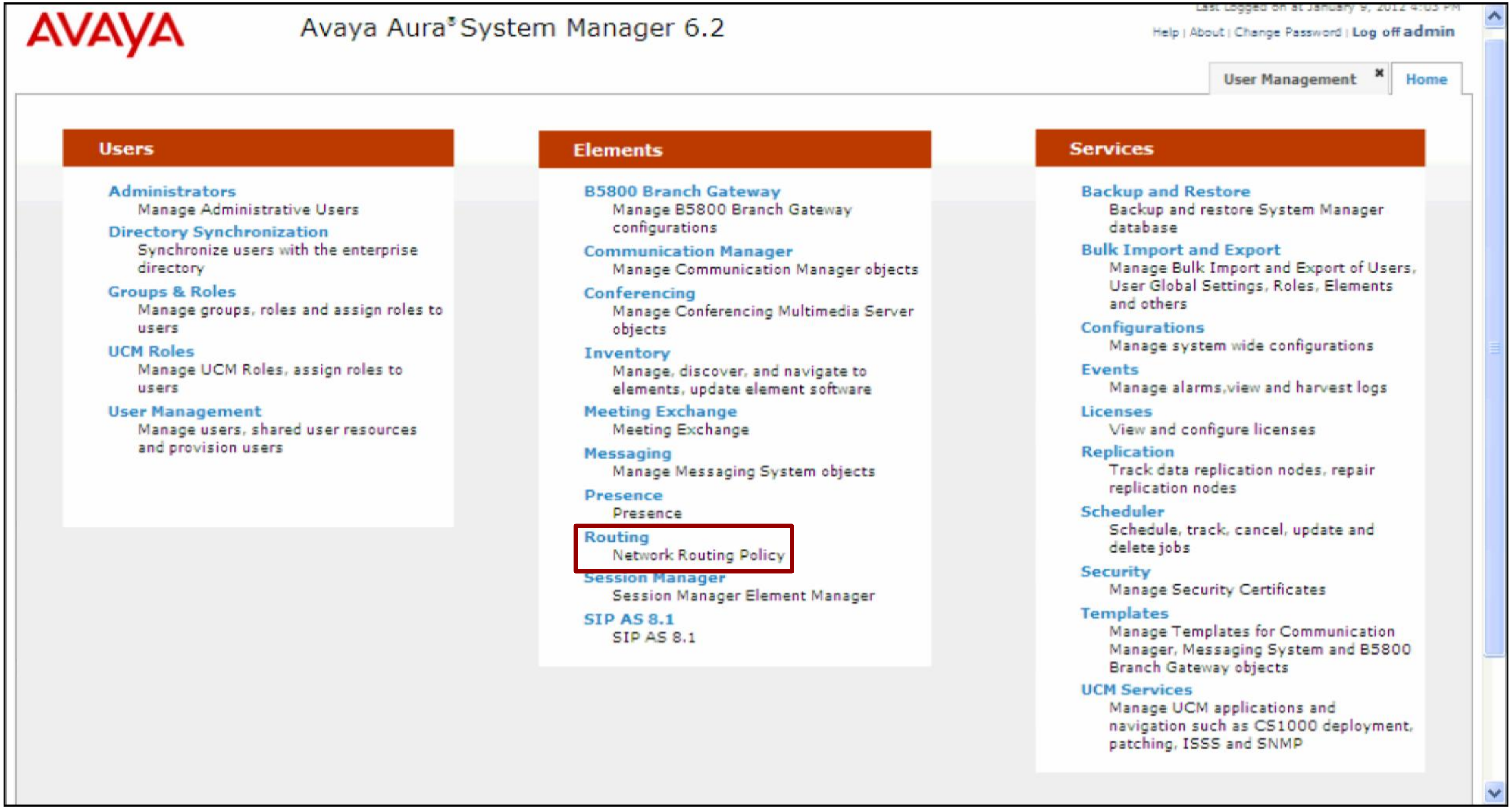
13.132.2.12

110.23.14.22

17.156.24.276

13.132.2.12 is a trusted source… Will process this request

SIP Entities (continued)



AVAYA Avaya Aura® System Manager 6.2

Last Logged on at January 9, 2012 4:03 PM

Help | About | Change Password | Log off admin

User Management ✖ | Home

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

UCM Roles
Manage UCM Roles, assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway configurations

Communication Manager
Manage Communication Manager objects

Conferencing
Manage Conferencing Multimedia Server objects

Inventory
Manage, discover, and navigate to elements, update element software

Meeting Exchange
Meeting Exchange

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

Scheduler
Schedule, track, cancel, update and delete jobs

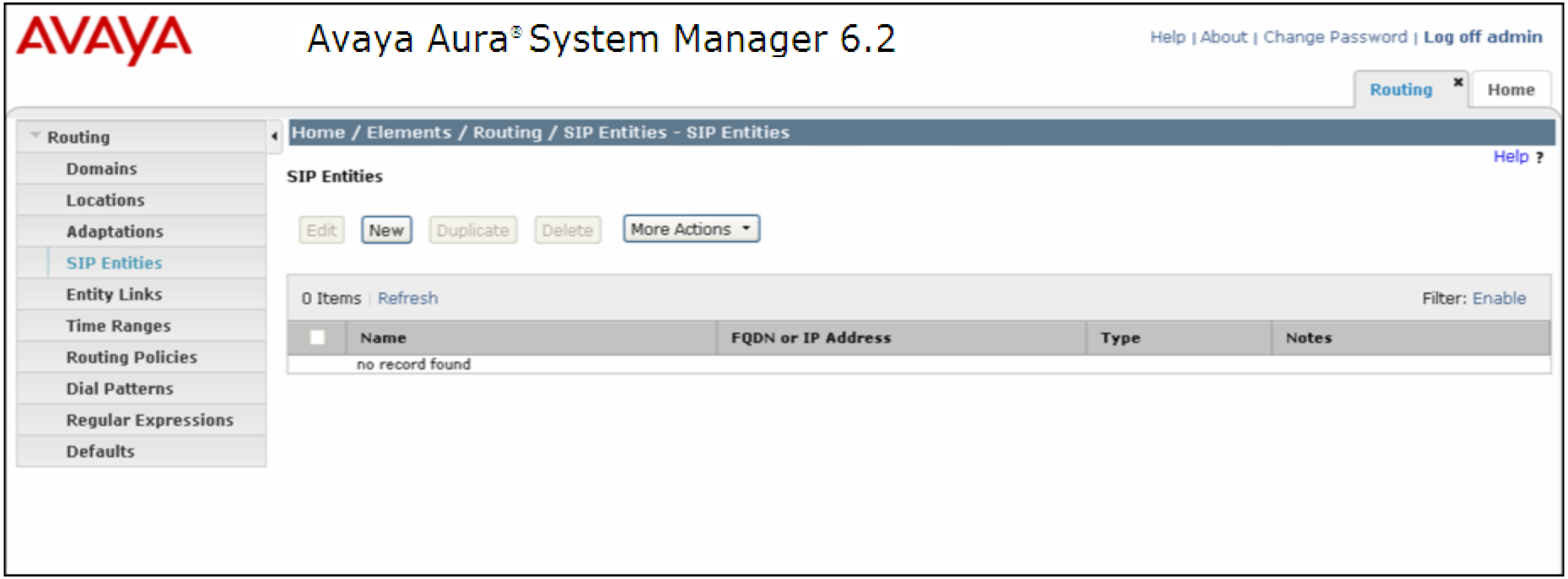
Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway objects

UCM Services
Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

SIP Entities (continued)

Routing >> SIP Entities



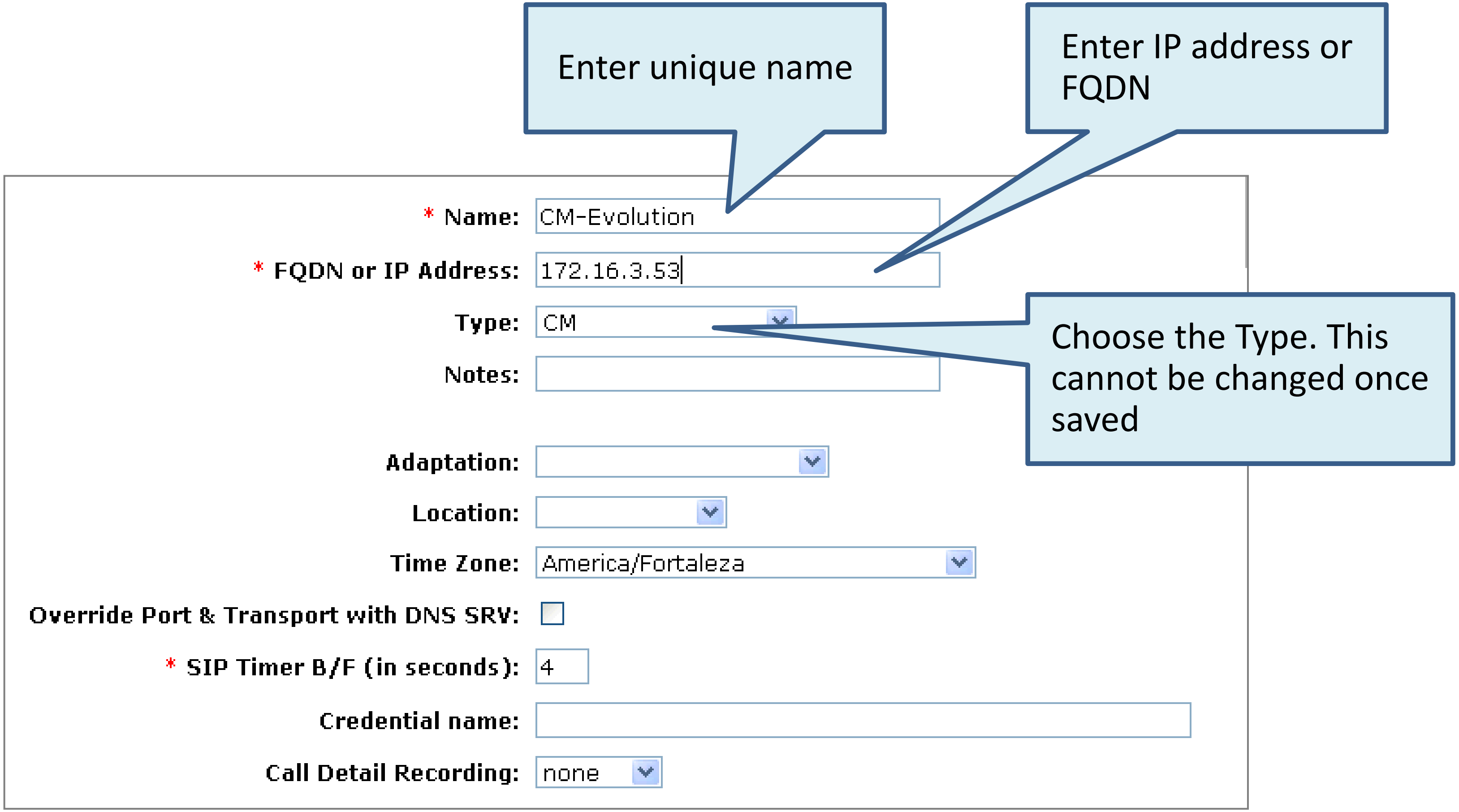
SIP Entities

0 Items

□	Name	FQDN or IP Address	Type	Notes
	no record found			

Select New

SIP Entities (continued)



* Name:	CM-Evolution
* FQDN or IP Address:	172.16.3.53
Type:	CM
Notes:	
Adaptation:	
Location:	
Time Zone:	America/Fortaleza
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

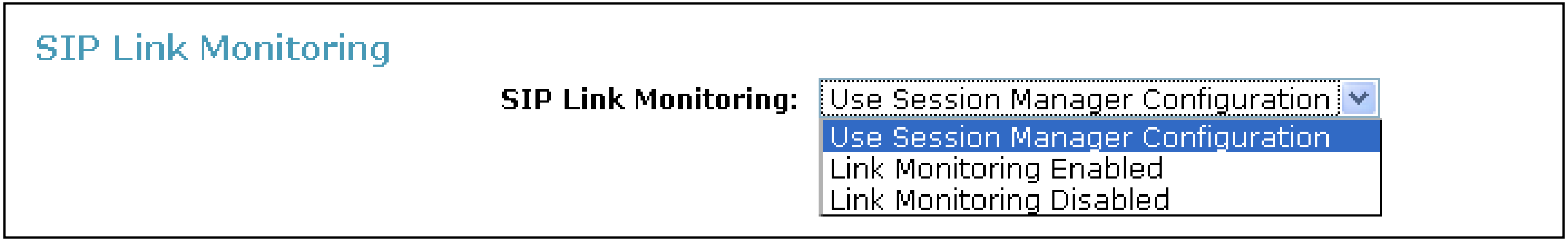
Enter unique name

Enter IP address or FQDN

Choose the Type. This cannot be changed once saved

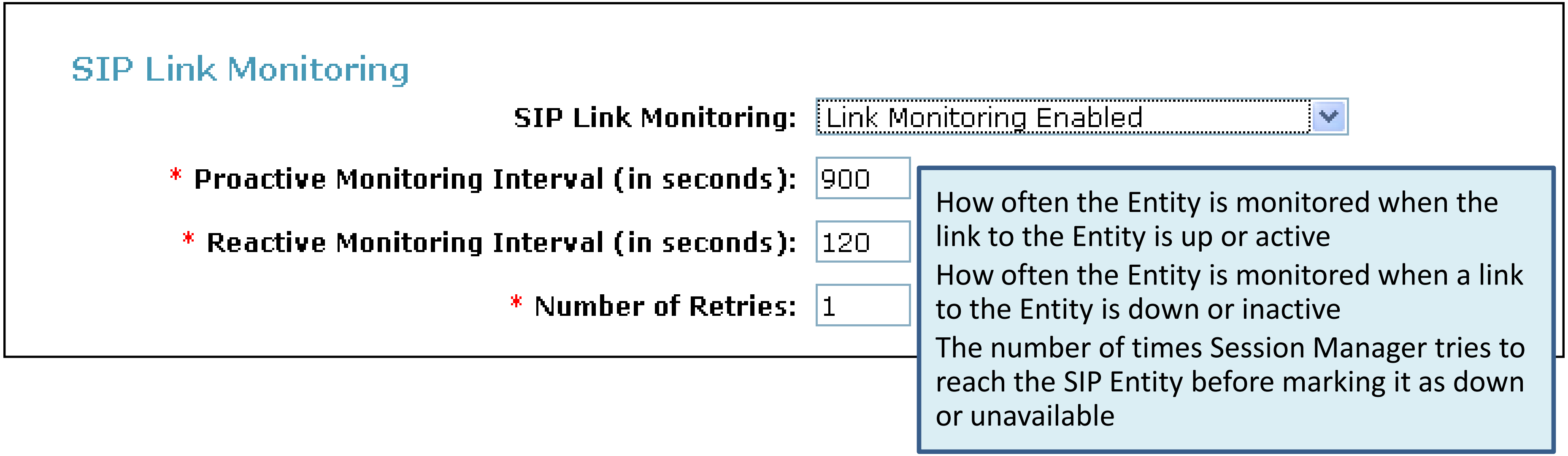
- Different fields will appear when adding a SIP entity other than Session Manager. They will be covered later when adding CM

SIP Entities (continued)



SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration



SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 900

* Reactive Monitoring Interval (in seconds): 120

* Number of Retries: 1

How often the Entity is monitored when the link to the Entity is up or active

How often the Entity is monitored when a link to the Entity is down or inactive

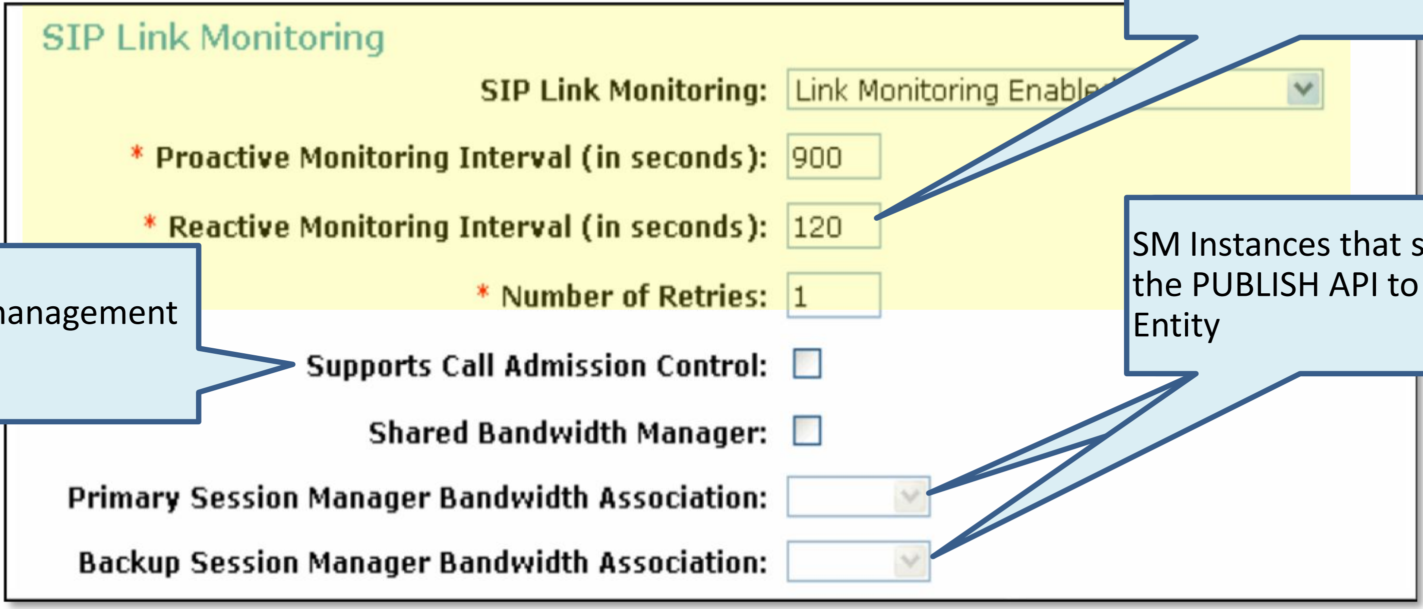
The number of times Session Manager tries to reach the SIP Entity before marking it as down or unavailable

Question: How does Session Manager monitor Entities?

Answer: Session Manager sends SIP OPTIONs messages.

SIP Entities (continued)

- 6.2 offers improved Call Admission Control for SIP Entities such as CM.
- This makes it possible for some Avaya Aura SIP Entities to take control over ALL of the bandwidth OR share it with Session Manager.



SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enable

* Proactive Monitoring Interval (in seconds): 900

* Reactive Monitoring Interval (in seconds): 120

* Number of Retries: 1

Supports Call Admission Control: □

Shared Bandwidth Manager: □

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

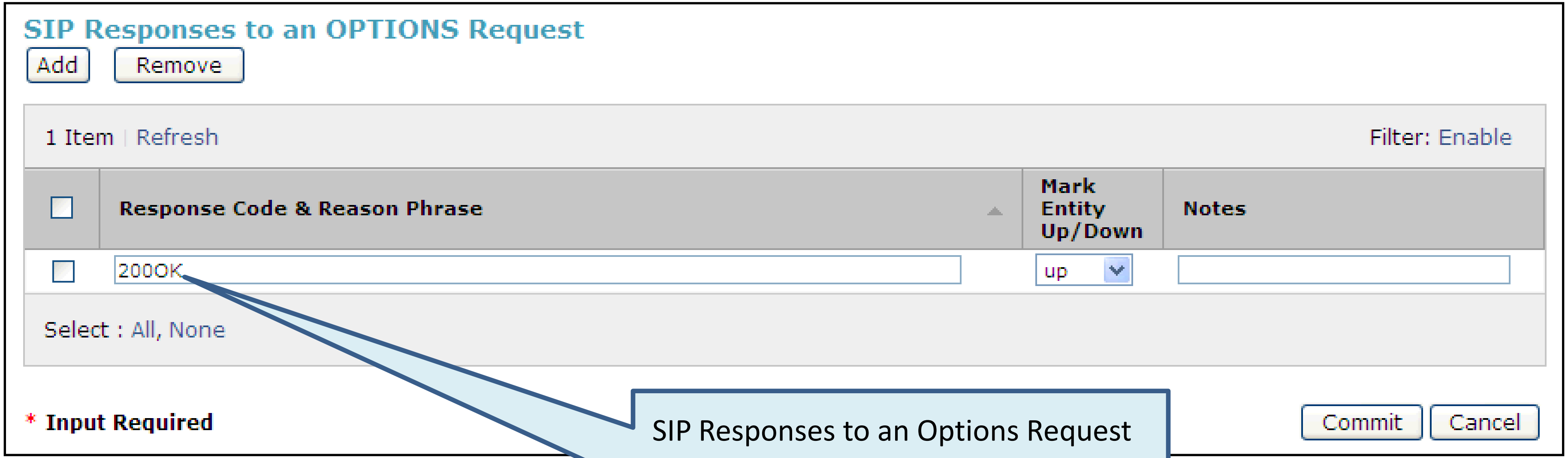
Enables CAC management for SIP Entity

Enables CAC management for SIP Entity

SM Instances that support the PUBLISH API to this SIP Entity

Handling Non-Standard Responses to OPTIONS Requests

- ASM 6.2 provides the ability to specify a SIP Response to an OPTIONS request for 3rd party SIP entities



SIP Responses to an OPTIONS Request

1 Item | Refresh   Filter: Enable

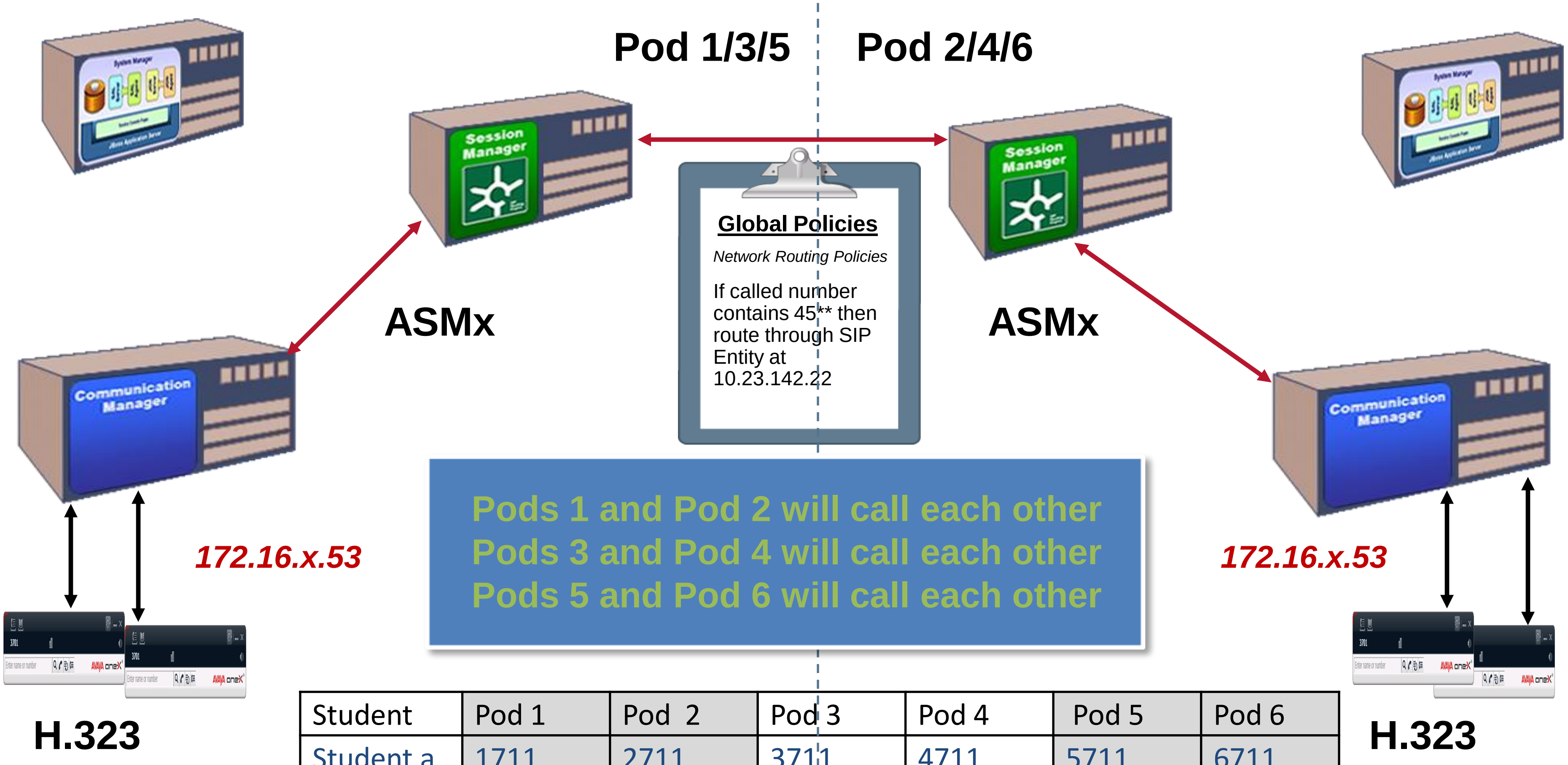
□	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
□	200OK	up	

Select : All, None

* **Input Required**

SIP Responses to an Options Request –
You can now you add a response to an OPTIONS message for 3rd party SIP Entities.

Routing Scenario: H.323 to H.323 Call Routing through Session Manager



Global Policies

Network Routing Policies

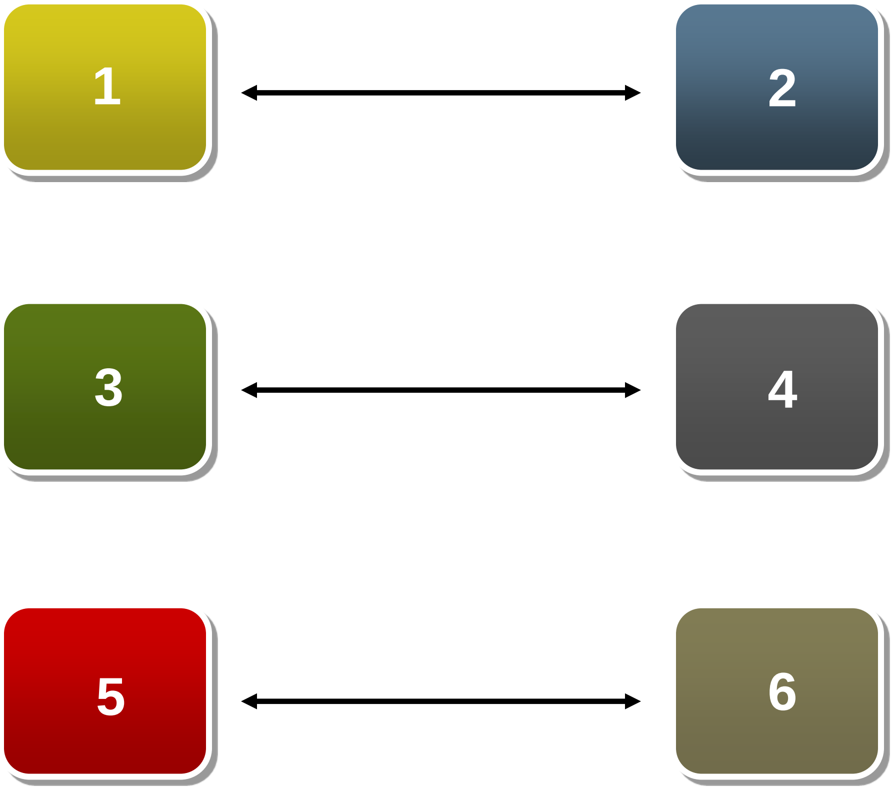
If called number contains 45** then route through SIP Entity at 10.23.142.22

Pods 1 and Pod 2 will call each other
Pods 3 and Pod 4 will call each other
Pods 5 and Pod 6 will call each other

Student	Pod 1	Pod 2	Pod 3	Pod 4	Pod 5	Pod 6
Student a	1711	2711	3711	4711	5711	6711
Student b	1721	2721	3721	4721	5721	6721

Pod Neighbors work together

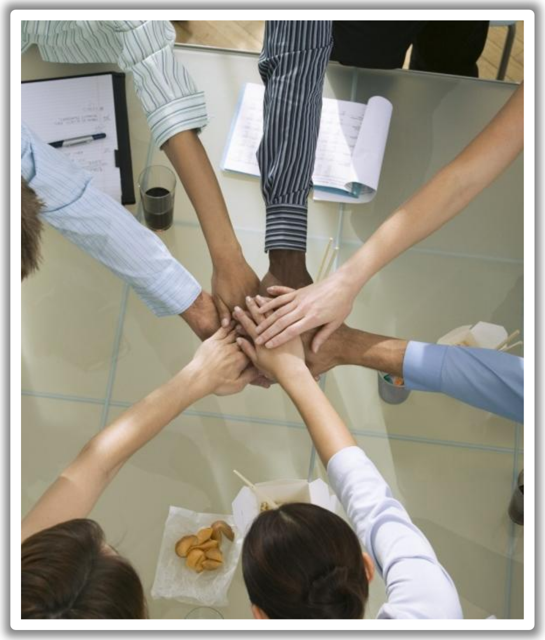
- Pod 1 works with Pod 2 and so on.



1 ↔ 2

3 ↔ 4

5 ↔ 6



For the next exercise, the following pods will be partnering up.

Exercise: Each Pod will define a SIP Entity for their CM

Objective: To support our first scenario, your CM will be added as a SIP Entity. **One** student from each Pod will define the SIP Entity for their Communication Manager the other student will watch.

Step	Action
1	Define one SIP Entity for CM
2	From the Routing Menu select SIP Entities
3	Select ***New***
4	Enter the name and IP Address for the CM. (refer to the Classroom Layout sheet on your desktop) **Student A creates: your CMx 172.16.x.53** **Student B shadows**
5	Select Type “**CM**”
6	Use the location: **Denver**
7	Time Zone: Select **America/Denver**
8	Use ‘***Session Manager Configuration***’ for SIP Link Monitoring. Let all other fields default.
9	Select ***Commit***

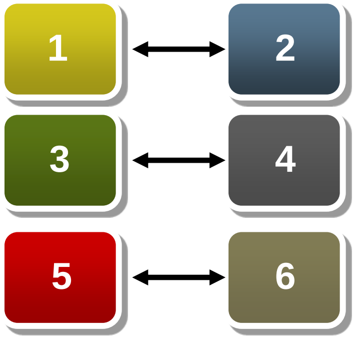
This exercise requires shadowing to be setup between students as one student will complete the exercise and the other student shadows.

Exercise: Add Pod Neighbor's ASM SIP Entity

Objective: Each pod will add 1 SIP Entitiy for the Pod Neighbor's ASM

Step	Action
1	Define a SIP Entity for your neighbors' ASM: (a SIP entity for your Pod partner was already created)
2	From the Routing Menu select SIP Entities
3	Select New
4	Enter the name **(ASMx)** and Eth2 SM100 IP Address for the ASM. (refer to the Classroom Layout sheet on your desktop)
5*	Select Type "**Other**" if the ASM is being managed by another System Manager
6	Use the location: **Denver**
7	Time Zone: **America/Denver**
8	Use '***Session Manager Configuration***' for SIP Link Monitoring. Let all other fields default.
9	Select ***Commit***

Pod Neighbors work together



For the next exercise, the following pods will be partnering up.

Entity Links

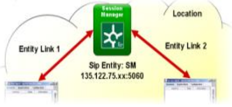
Creating Entity Links

Locations

Adaptations

SIP Entity

Entity Links



Time Ranges

SIP Domains

avaya.com
avaya.co.uk
avaya.co.sng
elsewhere.com

Dial Patterns

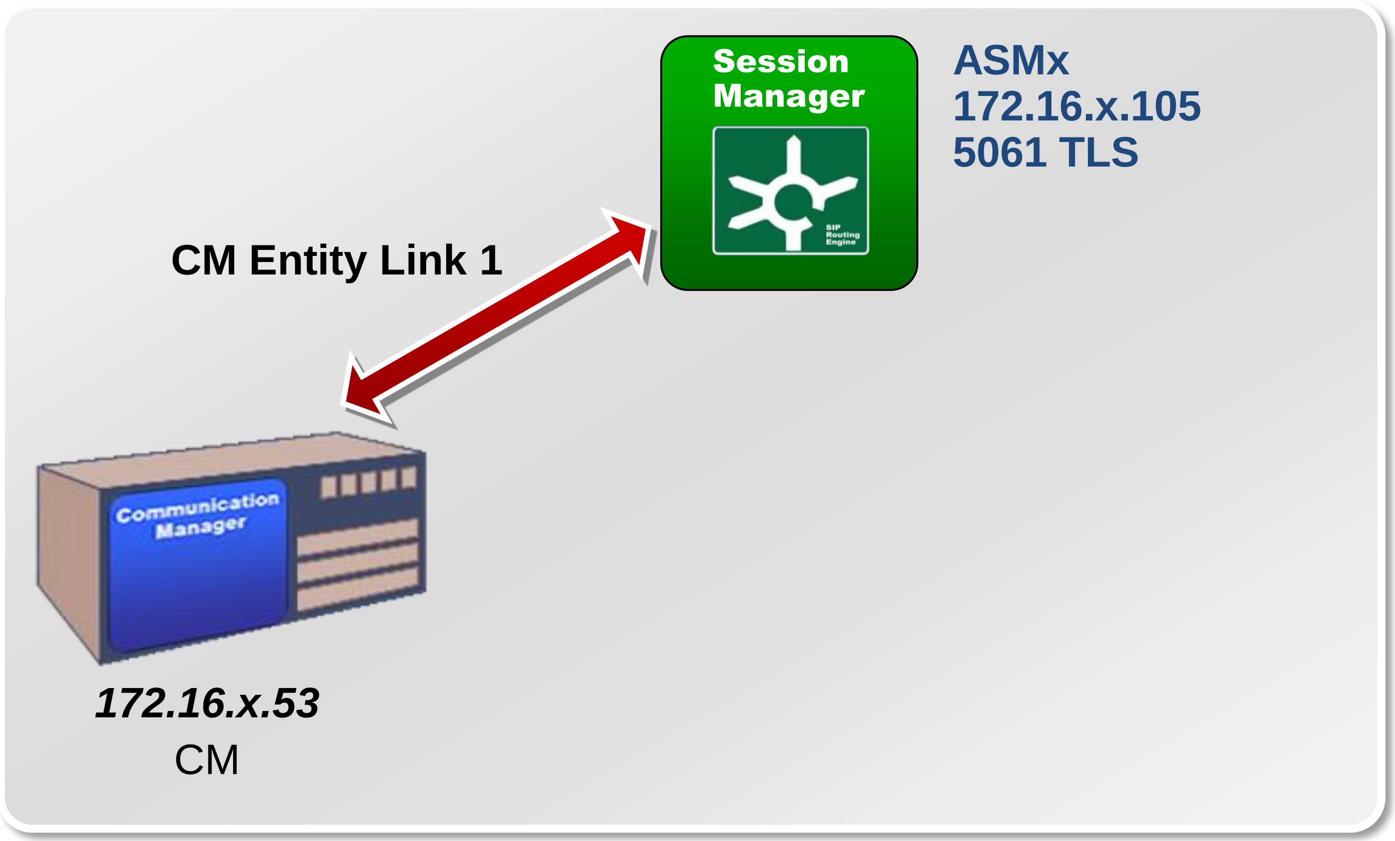
+44 to 00144
001 to +1
02920 to +442920
02920 to 001442920

Global Policies

Network Routing Policies

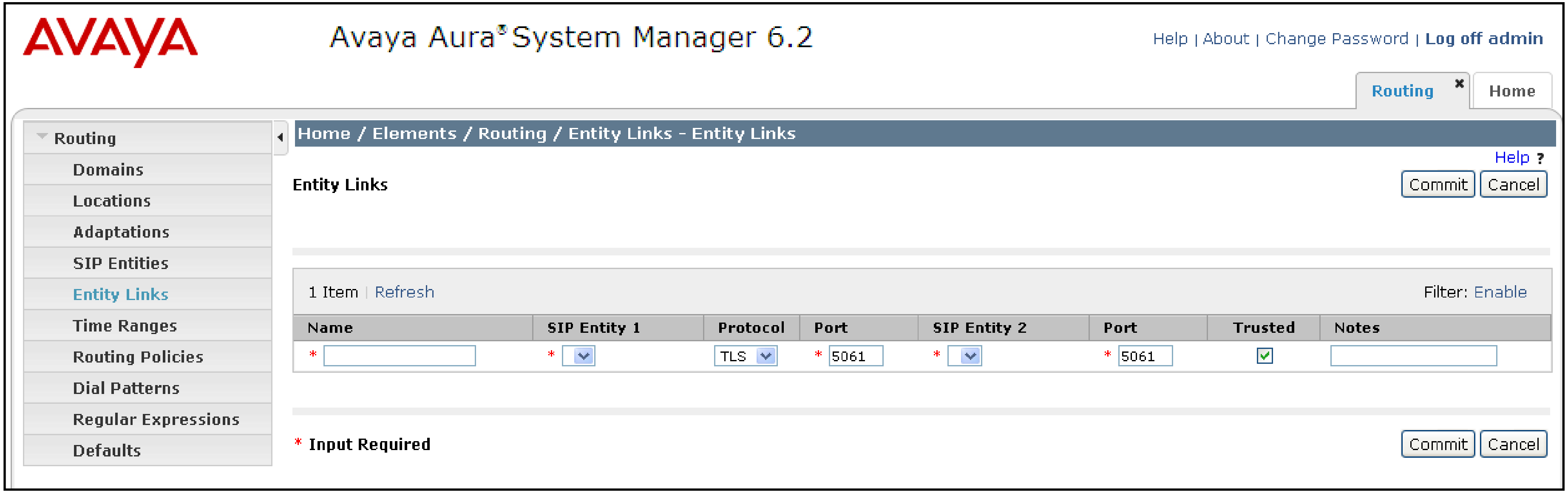
1. Destination SIP Entity
2. Time Ranges
3. Dial Patterns
4. Expressions

CM Entity Links



Session Manager requires a SIP Entity Link be created for every CM it will need to talk to directly.

Entity Links



Entity Links

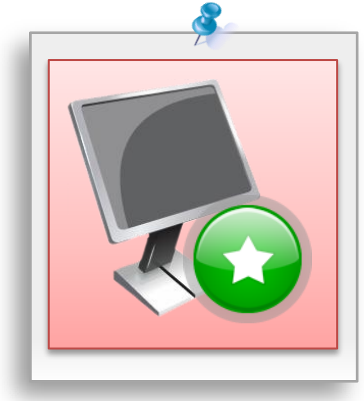
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
*	*	TLS	* 5061	*	* 5061	☑	

* Input Required

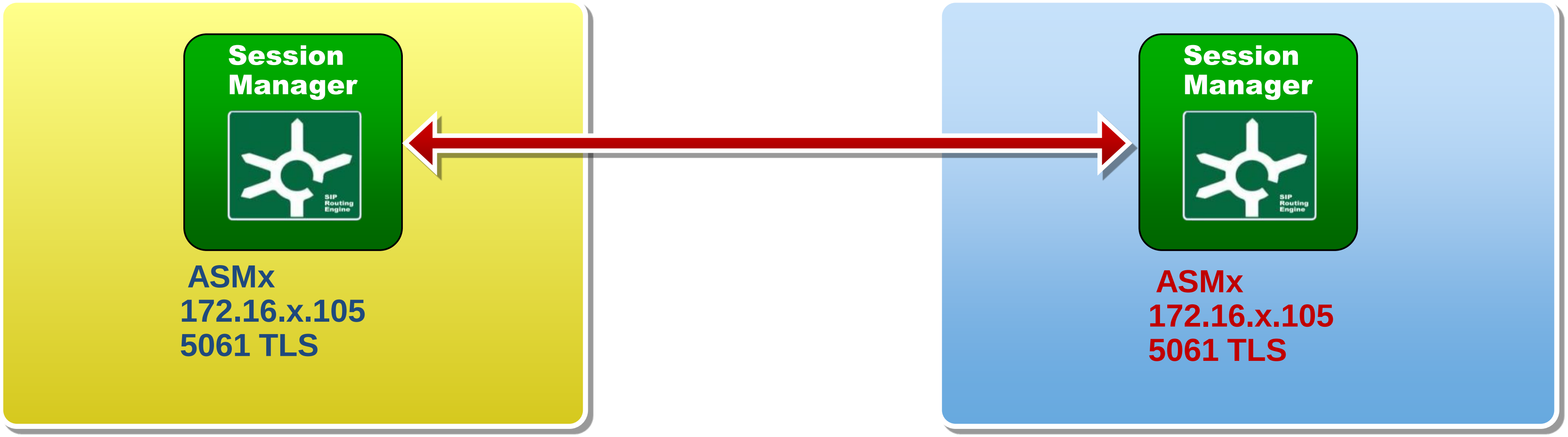
To be able to communicate with other SIP entities, Session Manager must know the port and the transport protocol.

Exercise: Define CM Entity Link

Step	Action
1	From the Routing Menu, select Entity Links
2	Select ***New***
3	Name : Your CM’s Entity Link : e.g: ASMx to My CM
4	**SIP Entity 1**: Select your Session Manager SIP Entity from the drop-down menu Protocol: **TLS** Port: **5061**
5	**SIP Entity 2**: **Your** CM Protocol: **TLS** Port: **5061** Trusted: leave check mark
6	Select ***Commit*** to save your changes



Session Manager Entity Links



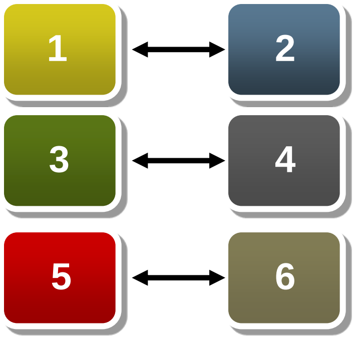
Session Manager requires a SIP Entity Link for every Session Manager it will communicate with.

Exercise: Define an Entity Link for pod neigbor’s ASM

Objective: Create an entity link from your Session Manager to your pod neighbor’s Session Manager.

Step	Action
1	From the Routing Menu, select Entity Links
2	Select New
3	Name : **Link to ASMx**
4	SIP Entity 1: Select your Session Manager SIP Entity from the drop-down menu Protocol: **TLS** Port: **5061**
5	SIP Entity 2: **ASMx** Port: **5061** Trusted: leave check mark
6	Select ***Commit*** to save your changes

Pod Neighbors work together

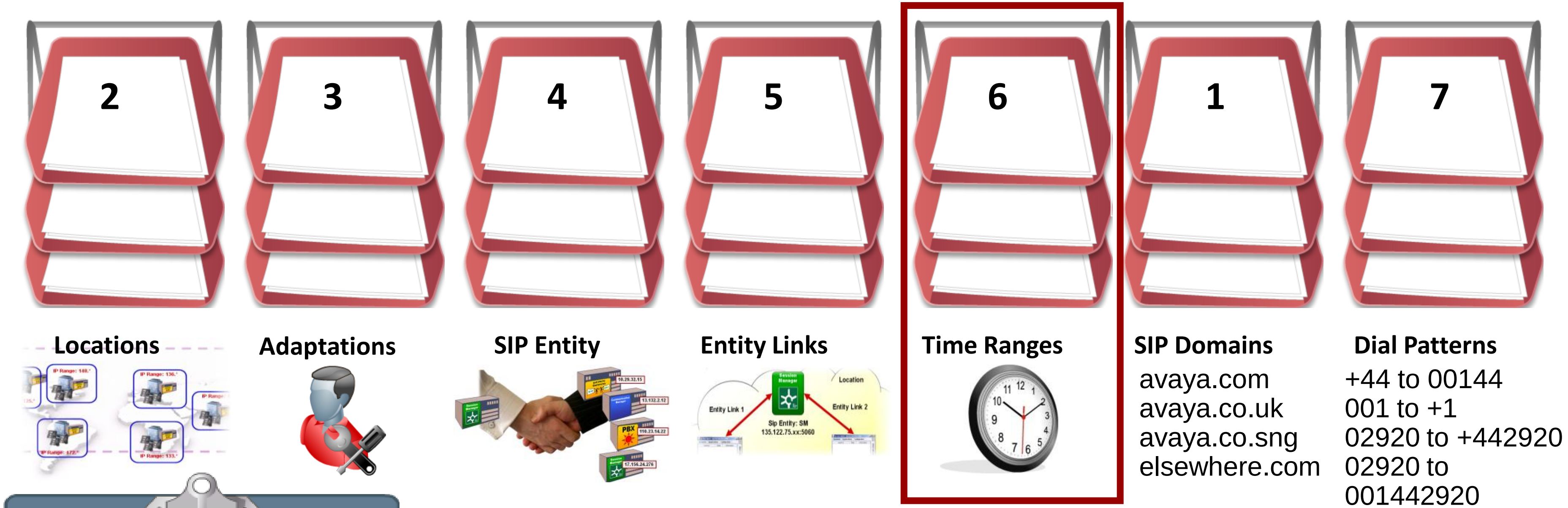


For the next exercise, the following pods will be partnering up.

AVAYA | LEARNING

Time Ranges

Creating Time Ranges



Locations

Adaptations

SIP Entity

Entity Links

Time Ranges

SIP Domains

avaya.com
avaya.co.uk
avaya.co.sng
elsewhere.com

Dial Patterns

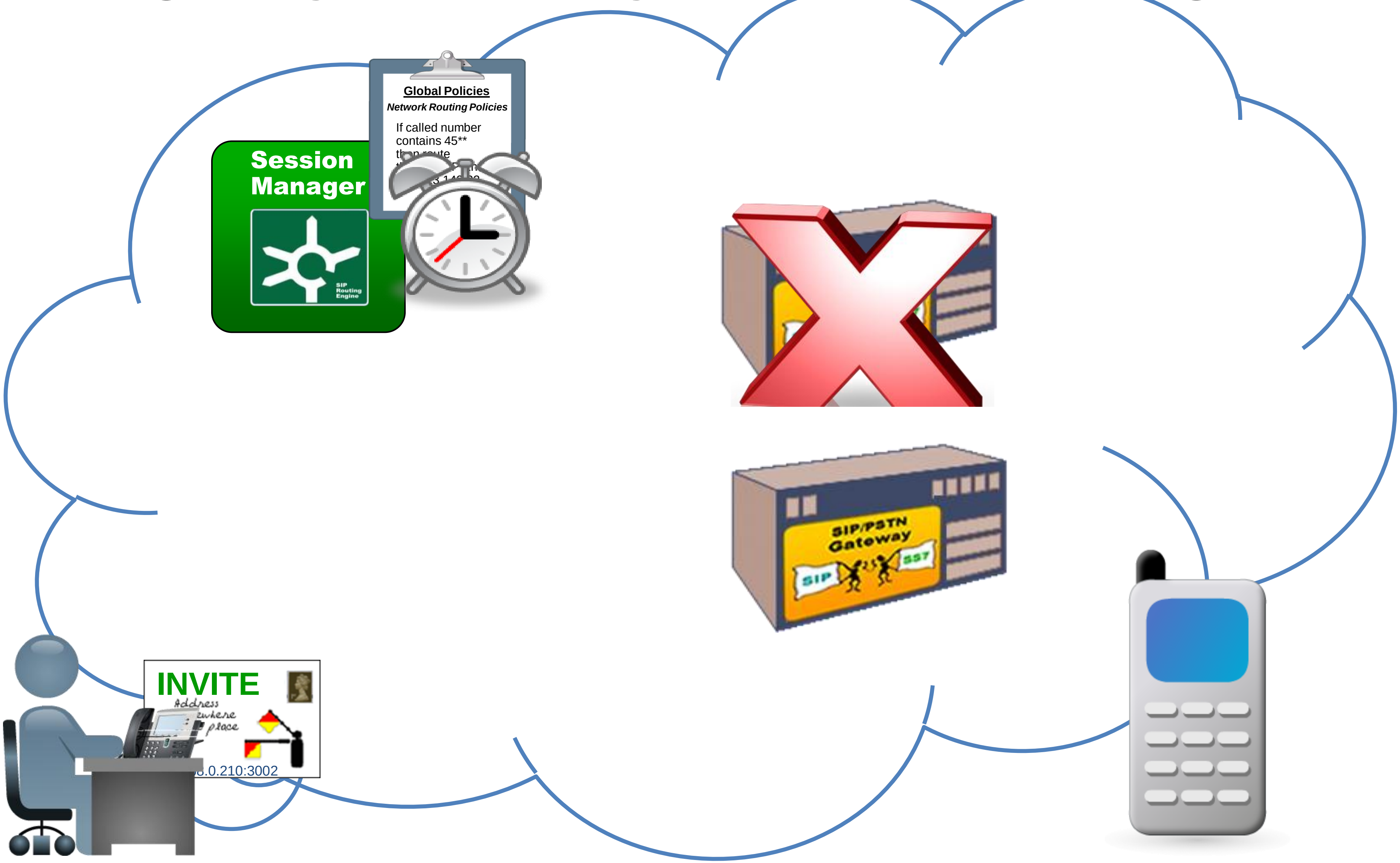
+44 to 00144
001 to +1
02920 to +442920
02920 to 001442920

Global Policies

Network Routing Policies

1. Destination SIP Entity
2. Time Ranges
3. Dial Patterns
4. Expressions

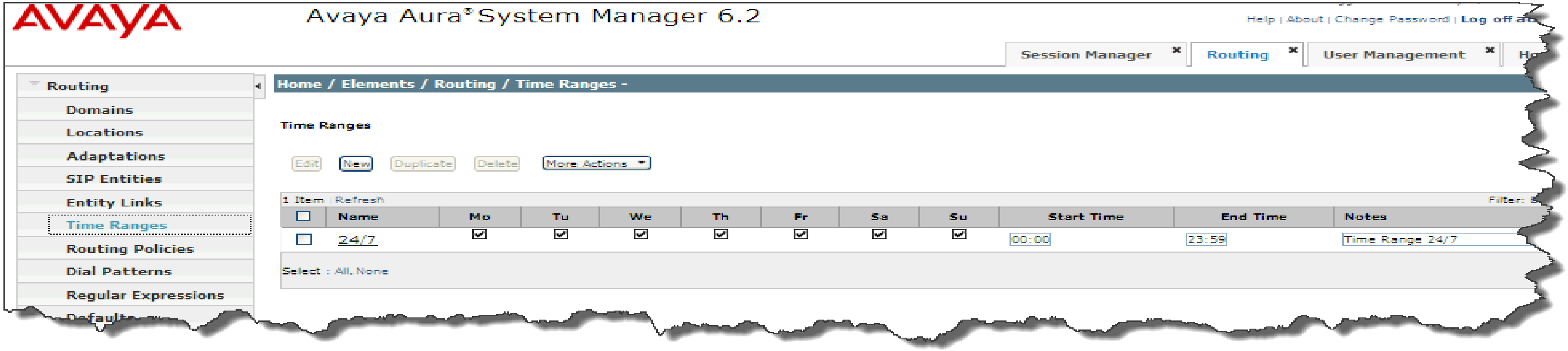
Routing Policy – Time of day and Least Cost Routing



Exercise: Define a Time Range

Step	Action
1	Student a: Define a Time Range that accepts calls Monday through Friday, 9 am to 5 pm. Name it **Workweek**
2	Student b: Define a Time Range that accepts calls all day Saturday and Sunday. Name it **Weekend**

Special Note: There is a 24/7 Time Range by default so it does not need to be created.



Home / Elements / Routing / Time Ranges -

Time Ranges

1 Item | Refresh

□	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
□	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

You must specify as many time ranges as necessary to cover all hours and days in a week for each administered routing policy.

Routing Policies

Creating Routing Policies

Locations

Adaptations

SIP Entity

Entity Links

Session Manager
Location
Entity Link 1
Entity Link 2
Sip Entity: SM
135.122.75.xx:5060

Time Ranges

SIP Domains

avaya.com
avaya.co.uk
avaya.co.sng
elsewhere.com

Dial Patterns

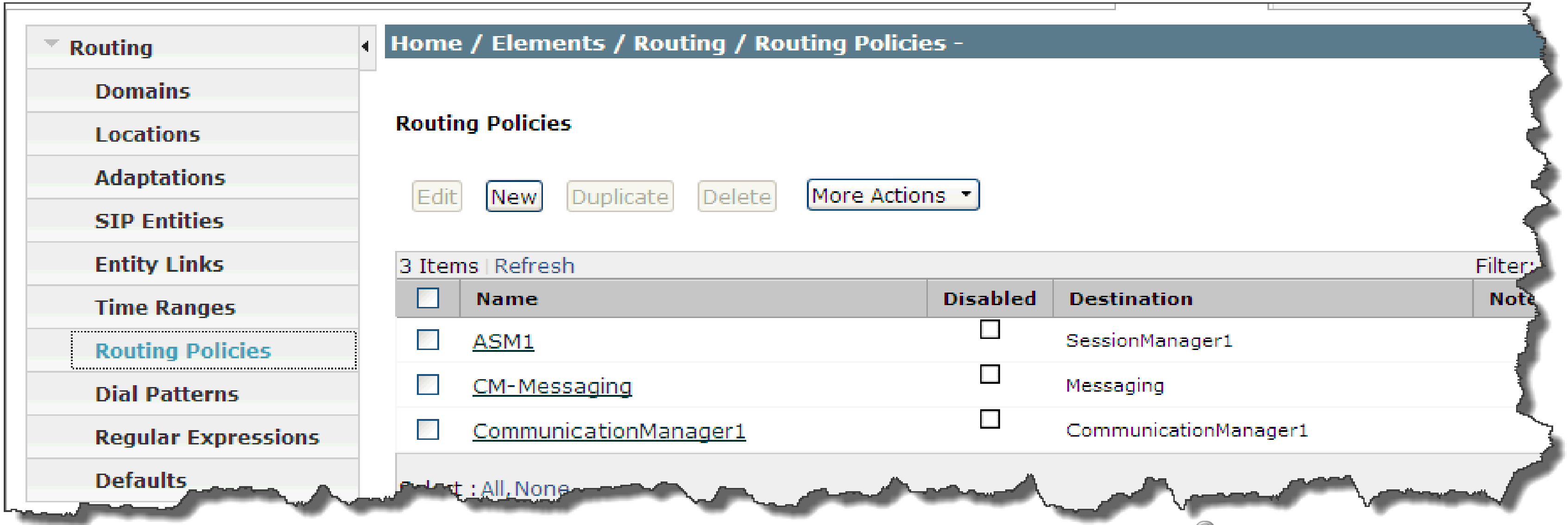
+44 to 00144
001 to +1
02920 to +442920
02920 to 001442920

<u>Global Policies</u>

Network Routing Policies

1. Destination SIP Entity
2. Time Ranges
3. Dial Patterns
4. Expressions

Routing Policies



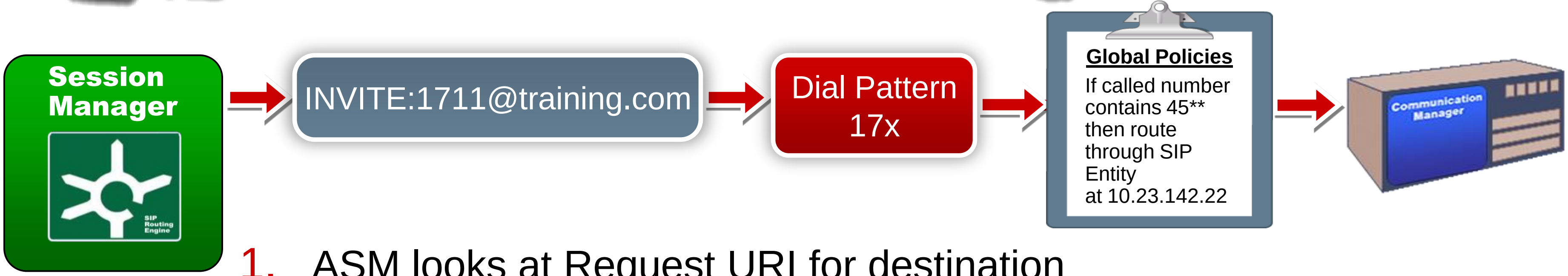
Home / Elements / Routing / Routing Policies -

Routing Policies

3 Items | Refresh   Filter:

□	Name	Disabled	Destination	Note
□	ASM1	□	SessionManager1	
□	CM-Messaging	□	Messaging	
□	CommunicationManager1	□	CommunicationManager1	

Select : All, None



Session Manager

INVITE:1711@training.com

Dial Pattern 17x

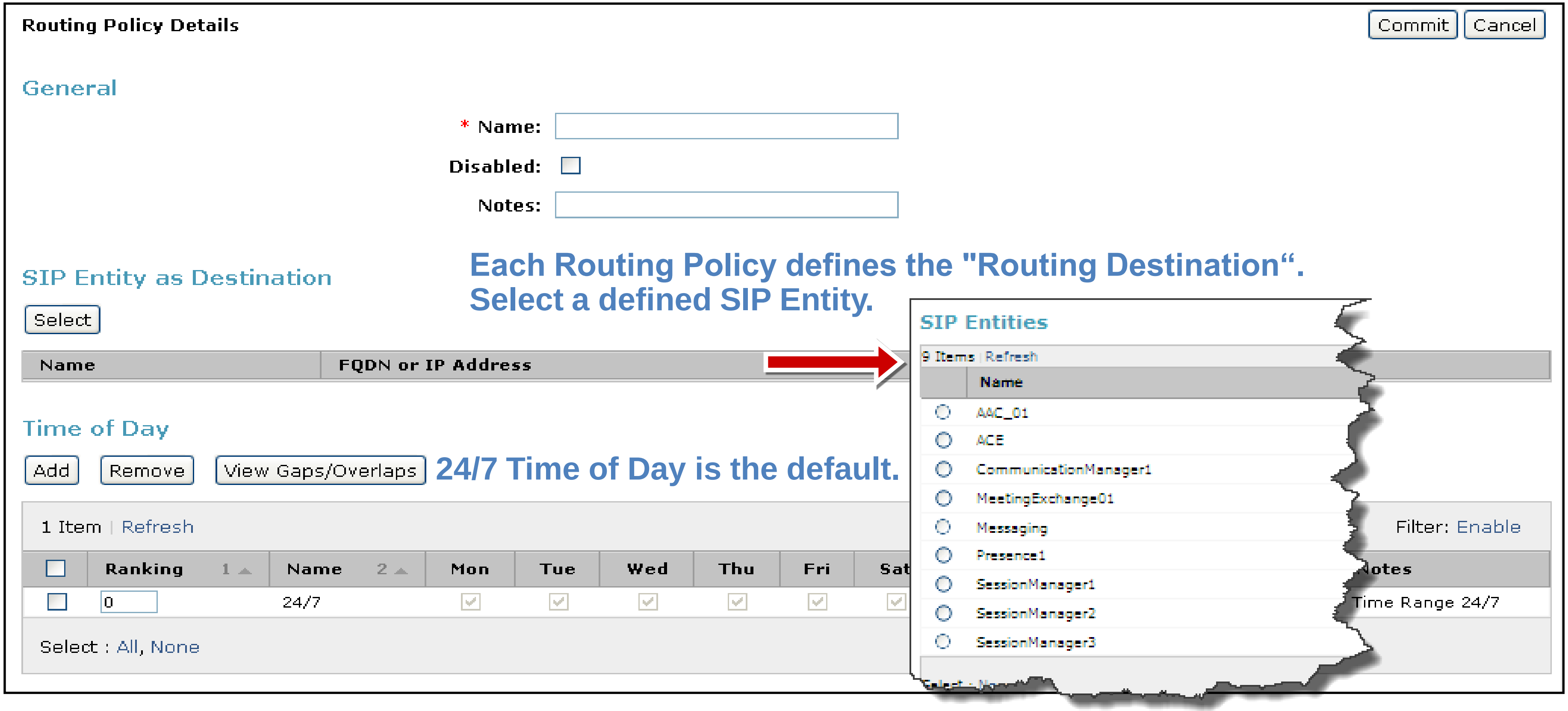
Global Policies

If called number contains 45** then route through SIP Entity at 10.23.142.22

1. ASM looks at Request URI for destination
2. Checks Dial Pattern/Regular Expressions for a match
3. Once it finds a match it uses the associated Routing Policy to route the call

Routing Policies (continued)

Each "Routing Policy" defines the "Routing Destination" (which is a "SIP Entity") as well as the "Time of Day" and its associated "Ranking".



Routing Policy Details

General

* Name:

Disabled: □

Notes:

SIP Entity as Destination

Name	FQDN or IP Address

Each Routing Policy defines the "Routing Destination“. Select a defined SIP Entity.

SIP Entities

9 Items | Refresh

	Name
○	AAC_01
○	ACE
○	CommunicationManager1
○	MeetingExchange01
○	Messaging
○	Presence1
○	SessionManager1
○	SessionManager2
○	SessionManager3

Time of Day

24/7 Time of Day is the default.

1 Item | Refresh

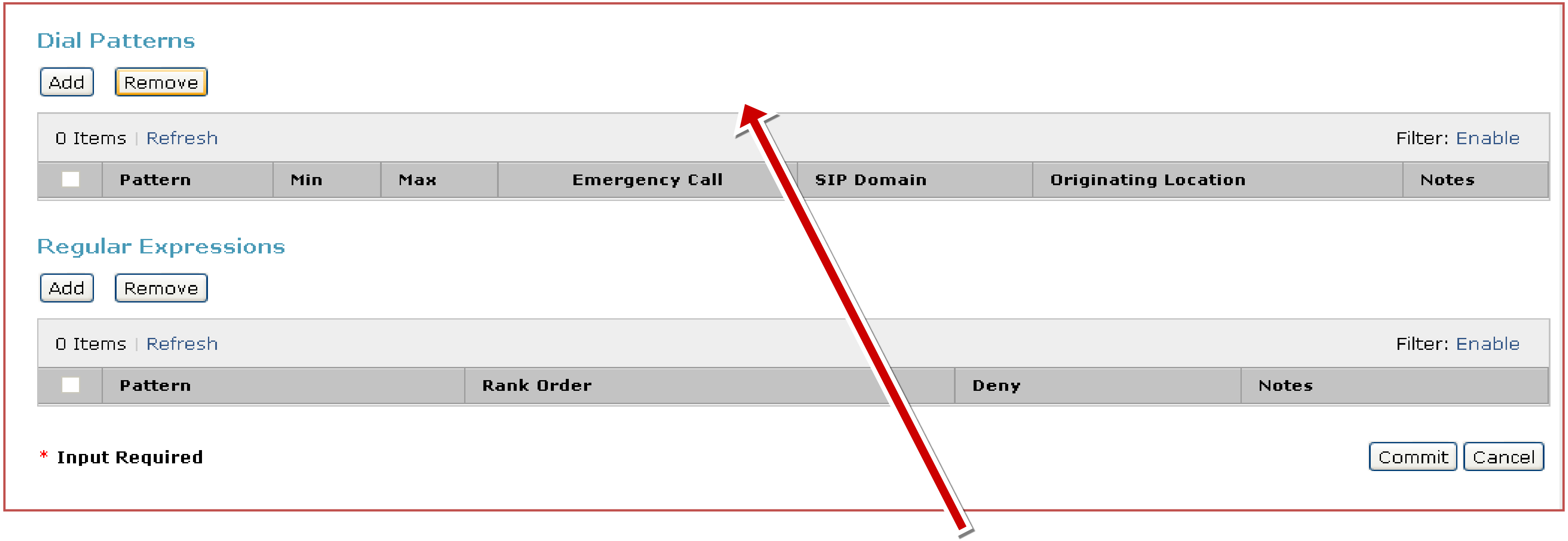
Filter: Enable

□	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Notes
□	0	24/7	✓	✓	✓	✓	✓	✓	Time Range 24/7

Select : All, None

Routing Policies (continued)

1. Save the new Routing Policy then define a new Dial Pattern or Regular Expression.
2. The Routing Policy can be assigned from within the Dial Pattern or Regular Expression page.



Dial Patterns

0 Items | Refresh Filter: Enable

□	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes

Regular Expressions

0 Items | Refresh Filter: Enable

□	Pattern	Rank Order	Deny	Notes

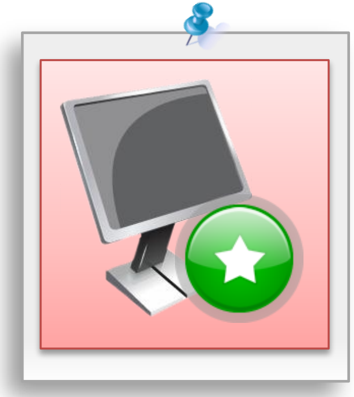
* Input Required

If a Dial Pattern or Expression does not already exist, it CANNOT be created in the Routing Policy page. Dial Patterns are created in the next step.

Exercise: Define (1) Routing Policy to Your CM

Objective: Define a Routing Policy to route calls to the Communication Managers

This is a shared exercise and will require students to shadow and view each other's changes.



Step	Action
1	Create (1) new Routing Policies. - One Student adds Routing Policy for your CM
2	Select **Routing Polices** from the Routing Menu
3	Enter Routing Policy **: RP to CMx**
4	Click on the **Select button** below ***SIP Entity as Destination.***
5	Select the radio button next to the CM SIP Entity. Click on the **Select** button.
6	**You can not pick a dial pattern yet. Leave at default.**
7	Select ***Commit*** to save your changes.

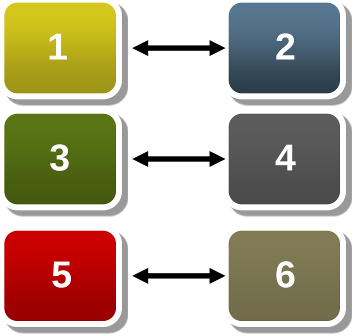
Exercise: Define Routing Policy to Neighbor's ASM's

Objective: Define a Routing Policy to route calls to the neighboring ASM.

Step	Action
1	Create a new Routing Policy for other Session Manager
2	Select **Routing Polices** from the Routing Menu
3	Enter Routing Policy Name **(example: RP to ASMx)**
4	Click on the **Select button** below ***SIP Entity as Destination.***
5	Select the radio button next to the ASM SIP Entity. Click on the **Select** button.
6	You can not pick a dial pattern yet. Leave at default.
7	Select ***Commit*** to save your changes.

172.16.x.105

Pod Neighbors work together

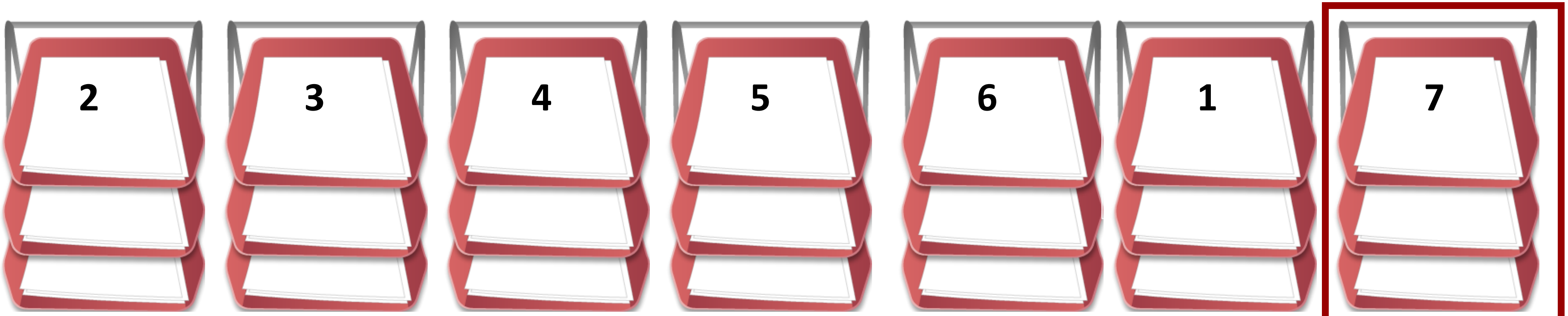


For the next exercise, the following pods will be partnering up.

AVAYA | LEARNING

Dial Patterns

Dial Patterns



Locations

Adaptations

SIP Entity

Entity Links

Time Ranges

SIP Domains

avaya.com
avaya.co.uk
avaya.co.sng
elsewhere.com

Dial Patterns

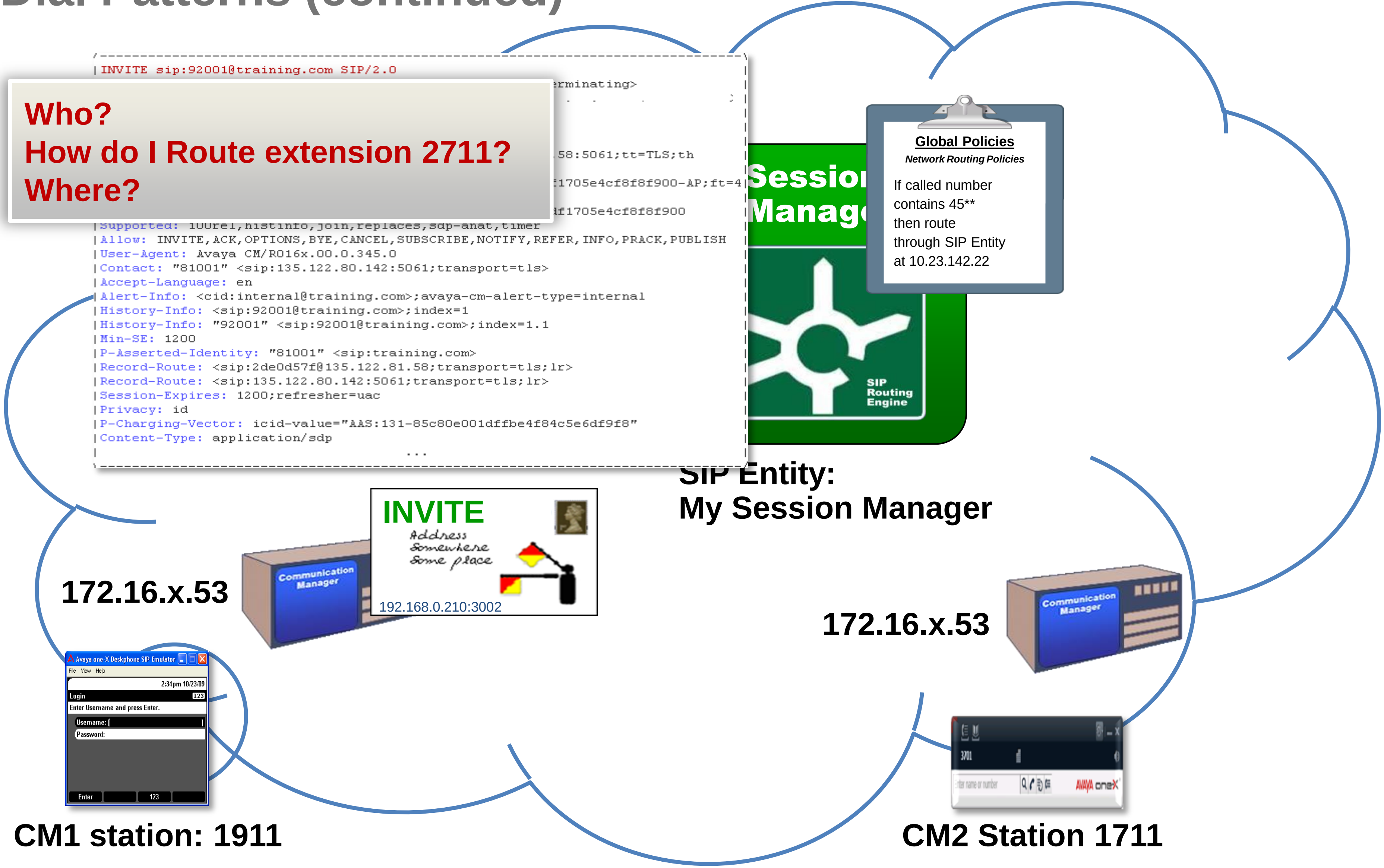
+44 to 00144
001 to +1
02920 to +442920
02920 to 001442920

Global Policies

Network Routing Policies

1. Destination SIP Entity
2. Time Ranges
3. Dial Patterns
4. Expressions

Dial Patterns (continued)



Who?
How do I Route extension 2711?
Where?

```
INVITE sip:92001@training.com SIP/2.0
                                                   erminating>
                                                   .58:5061;tt=TLS;th
                                                   f1705e4cf8f8f900-AP;ft=4
                                                   df1705e4cf8f8f900
Supported: 100rel,histinfo,join,replaces,sdp-anat,timer
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,INFO,PRACK,PUBLISH
User-Agent: Avaya CM/R016x.00.0.345.0
Contact: "81001" <sip:135.122.80.142:5061;transport=tls>
Accept-Language: en
Alert-Info: <cid:internal@training.com>;avaya-cm-alert-type=internal
History-Info: <sip:92001@training.com>;index=1
History-Info: "92001" <sip:92001@training.com>;index=1.1
Min-SE: 1200
P-Asserted-Identity: "81001" <sip:training.com>
Record-Route: <sip:2de0d57f@135.122.81.58;transport=tls;lr>
Record-Route: <sip:135.122.80.142:5061;transport=tls;lr>
Session-Expires: 1200;refresher=uac
Privacy: id
P-Charging-Vector: icid-value="AAS:131-85c80e001dffbe4f84c5e6df9f8"
Content-Type: application/sdp
                                   ...
```

Global Policies

Network Routing Policies

If called number
contains 45**
then route
through SIP Entity
at 10.23.142.22

SIP Entity:
My Session Manager

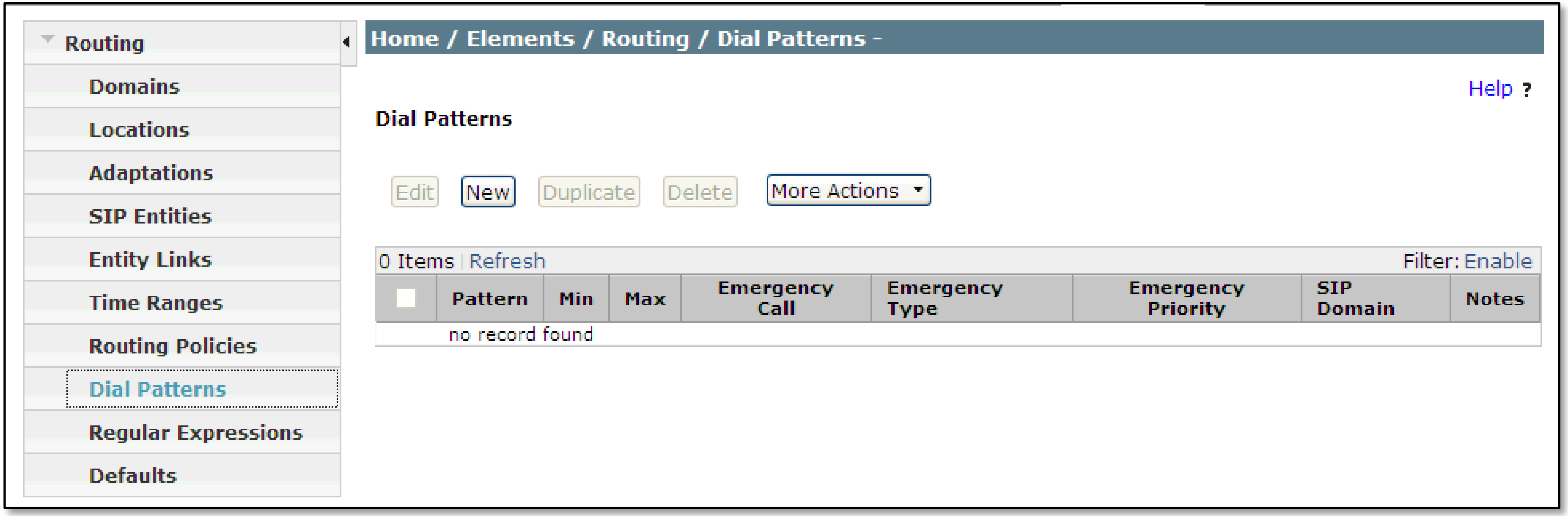
172.16.x.53

172.16.x.53

CM1 station: 1911

CM2 Station 1711

Dial Patterns (continued)



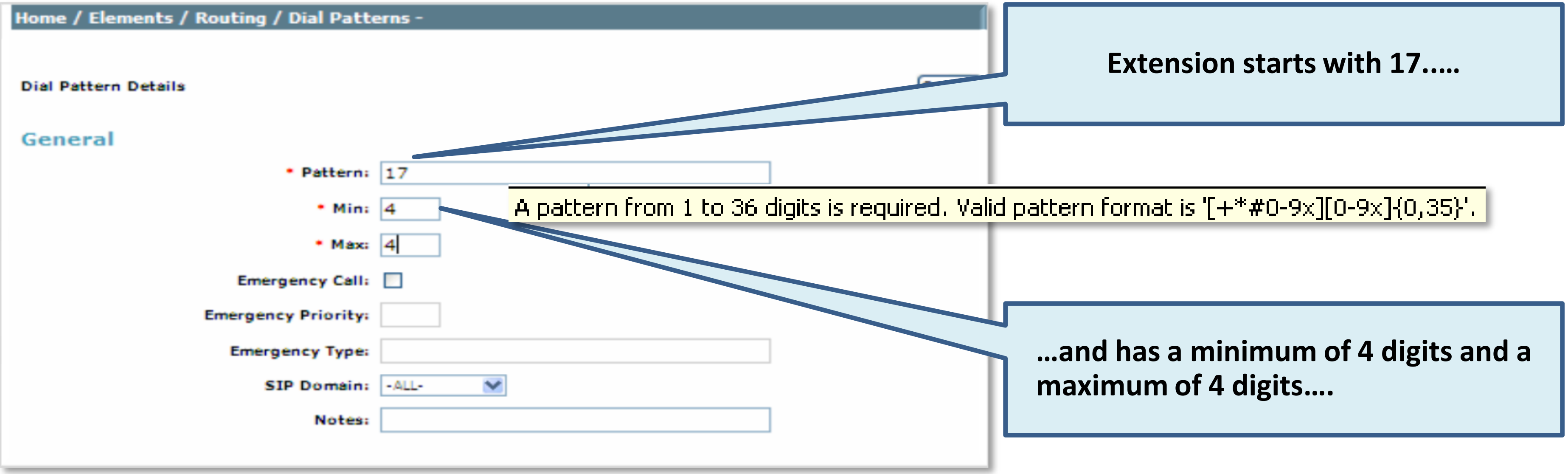
Dial Patterns

0 Items | Refresh Filter: Enable

□	Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
	no record found							

A dial pattern specifies which routing policy is used to route a call based on matching the digits dialed by a user.

Dial Pattern (continued)



Home / Elements / Routing / Dial Patterns -

Dial Pattern Details

General

- * Pattern: 17
- * Min: 4
- * Max: 4
- Emergency Call: □
- Emergency Priority:
- Emergency Type:
- SIP Domain: -ALL-
- Notes:

A pattern from 1 to 36 digits is required. Valid pattern format is '[+*#0-9x][0-9x]{0,35}'.

Extension starts with 17.....

...and has a minimum of 4 digits and a maximum of 4 digits....

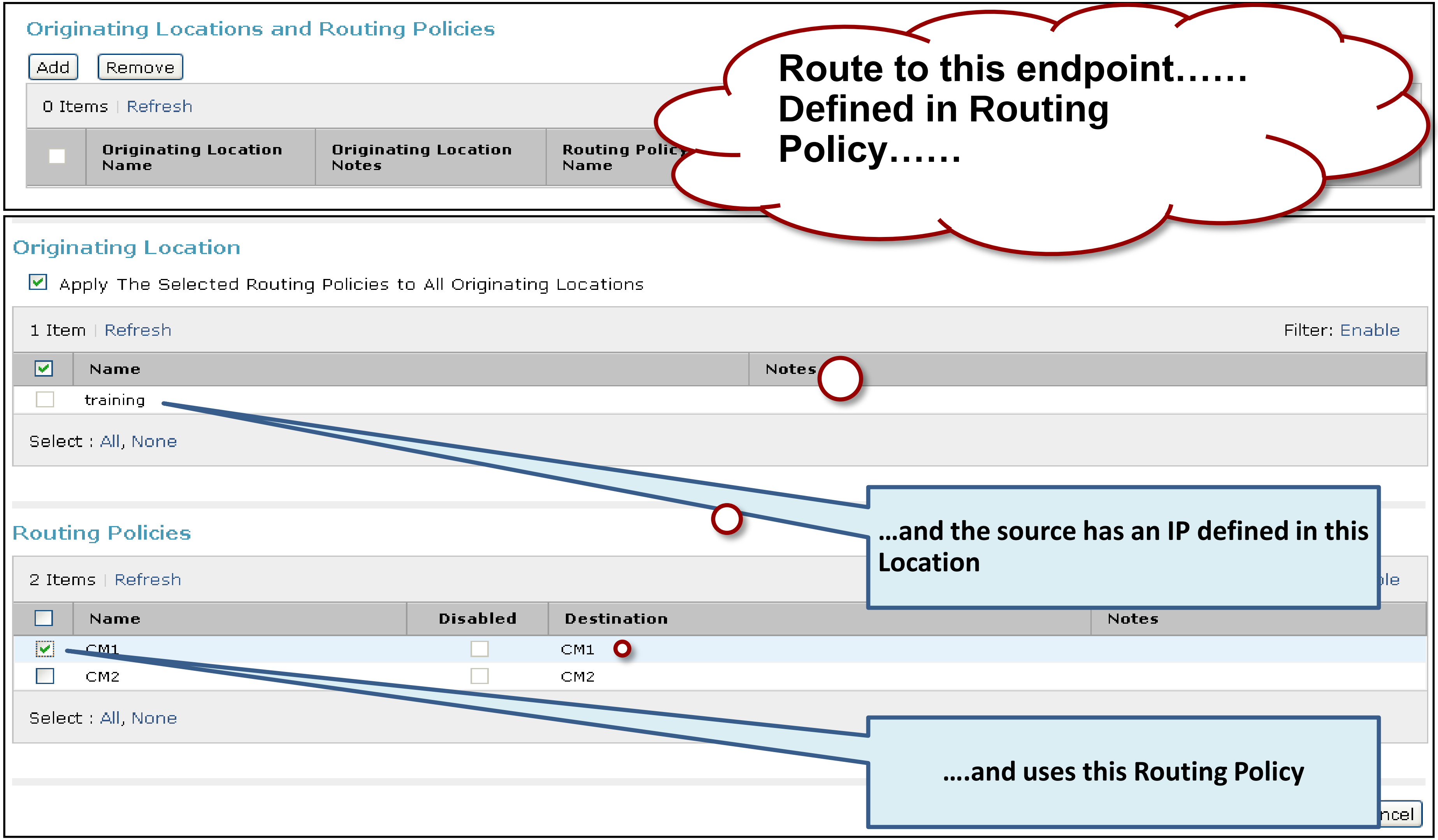
Pattern:

- Valid digits are 0-9
- Valid characters for the leading position are,+, *, and #
- x (lowercase only) is a wildcard character
- White spaces are not allowed.
- * and # are not wildcards as they can be part of the Dial Pattern

Longer matches get a higher priority over shorter matches.
For example, +1601555 has a higher priority as compared to +1601.

For matches of equal length, exact matches have a higher priority over wildcard matches.
For example, +1601555 has a higher priority as compared to +1xxx555.

Dial Pattern (continued)



Originating Locations and Routing Policies

0 Items | Refresh

□	Originating Location Name	Originating Location Notes	Routing Polic

Route to this endpoint……
Defined in Routing Policy……

Originating Location

☑ Apply The Selected Routing Policies to All Originating Locations

1 Item | Refresh   Filter: Enable

☑	Name	Notes
□	training	

Select : All, None

…and the source has an IP defined in this Location

Routing Policies

2 Items | Refresh   ble

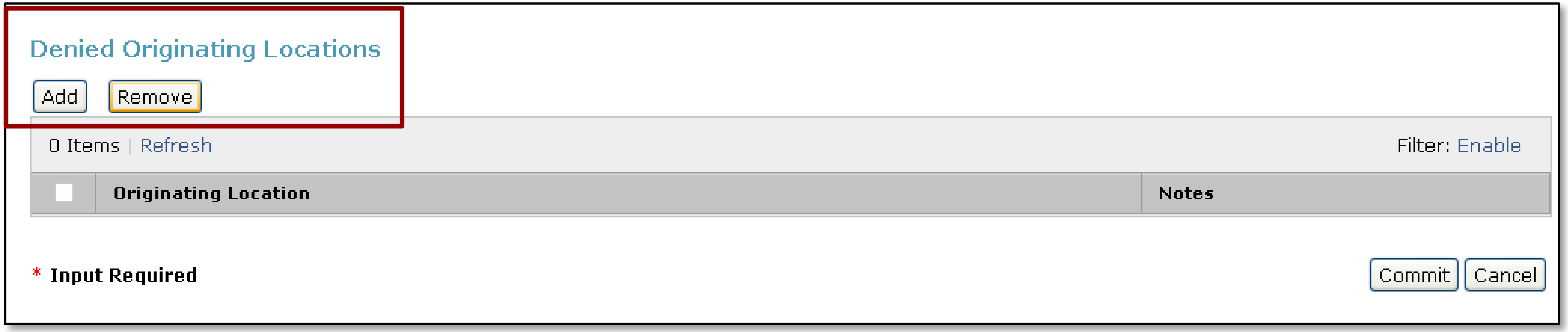
□	Name	Disabled	Destination	Notes
☑	CM1	□	CM1	
□	CM2	□	CM2	

Select : All, None

….and uses this Routing Policy

Dial Pattern (continued)

You can block processing of calls from some or ALL

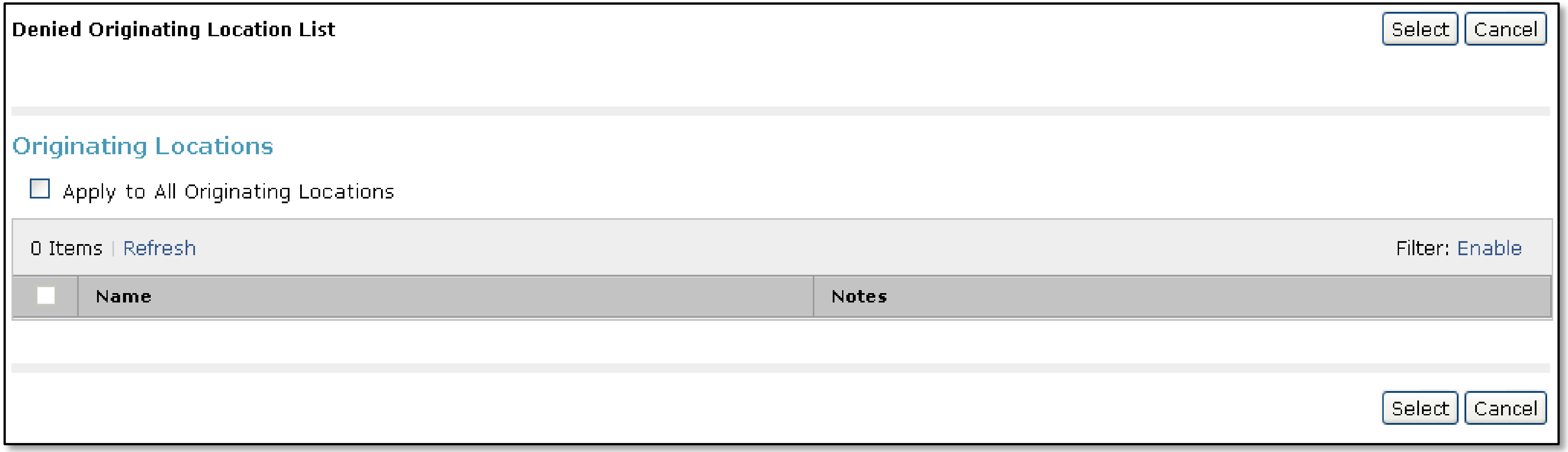


Denied Originating Locations

0 Items | Refresh   Filter: Enable

□	Originating Location	Notes

* **Input Required**



Denied Originating Location List

Originating Locations

□ Apply to All Originating Locations

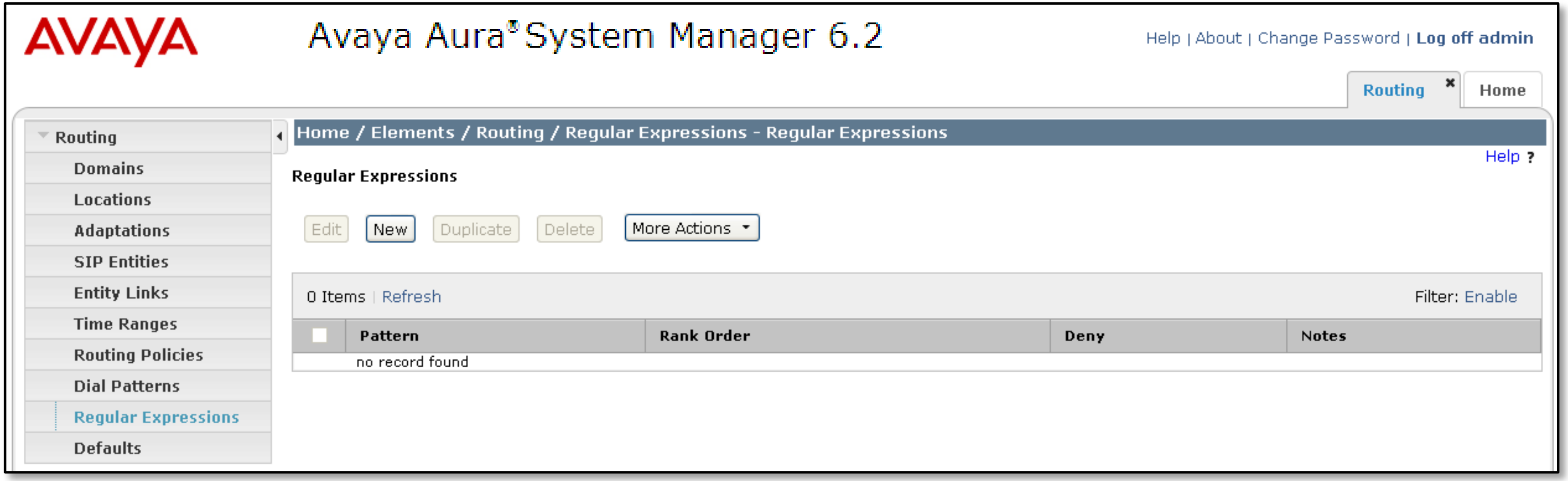
0 Items | Refresh   Filter: Enable

□	Name	Notes

AVAYA | LEARNING

Regular Expressions

Regular Expressions



Regular Expressions

□	Pattern	Rank Order	Deny	Notes
	no record found			

Regular Express enables use of:

1. **Alpha-numeric characters**
2. **Wildcards**

"*" matches any character string.

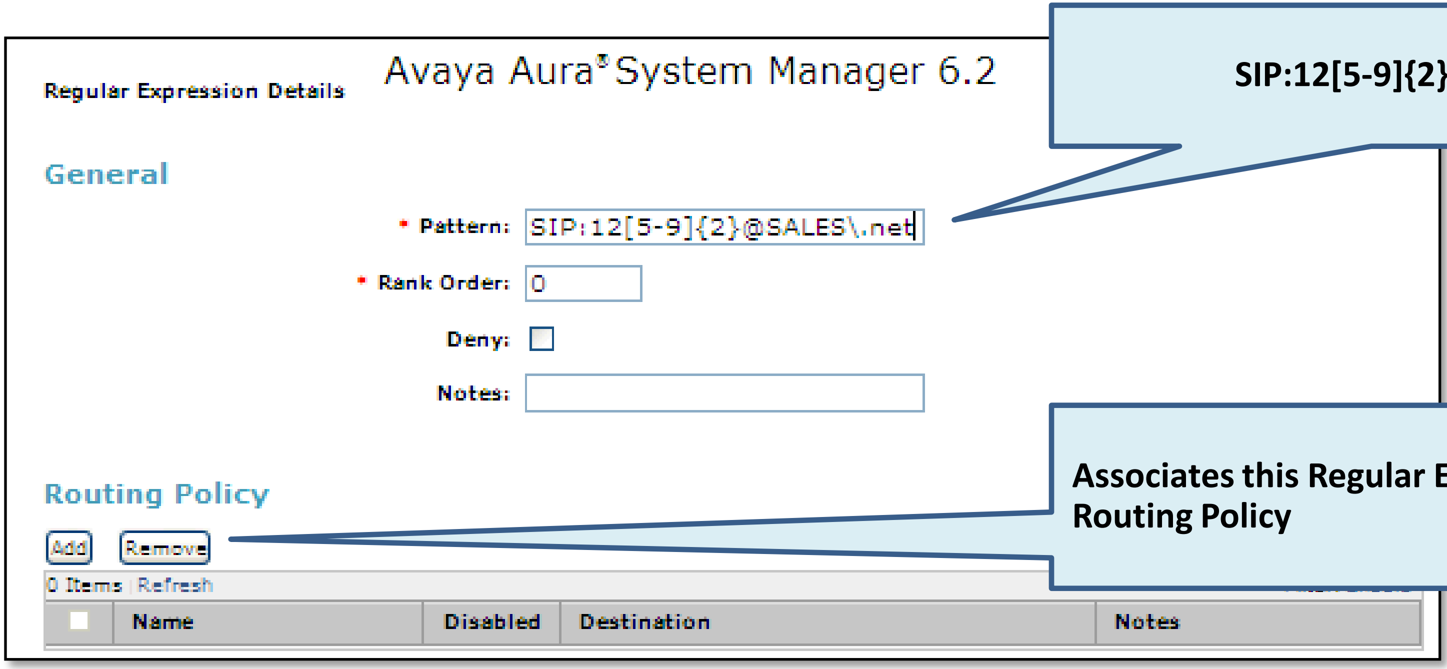
"." matches one character.

"\ " makes a character lose its special meaning

Some examples are:

- For “www.SIPentity.domain.com”, use the string “www\.SIPentity\.domain\.com”
- For “192.14.11.22”, use string “192\.14\.11\.22”.
  - The routing policy with a regular expression .*@.*\.de routes all calls requesting a domain in Germany (for example, name@company.de) to a Frankfurt Gateway.

Regular Expressions (continued)



Regular Expression Details

Avaya Aura® System Manager 6.2

General

* Pattern: SIP:12[5-9]{2}@SALES\.net

* Rank Order: 0

Deny: □

Notes:

Routing Policy

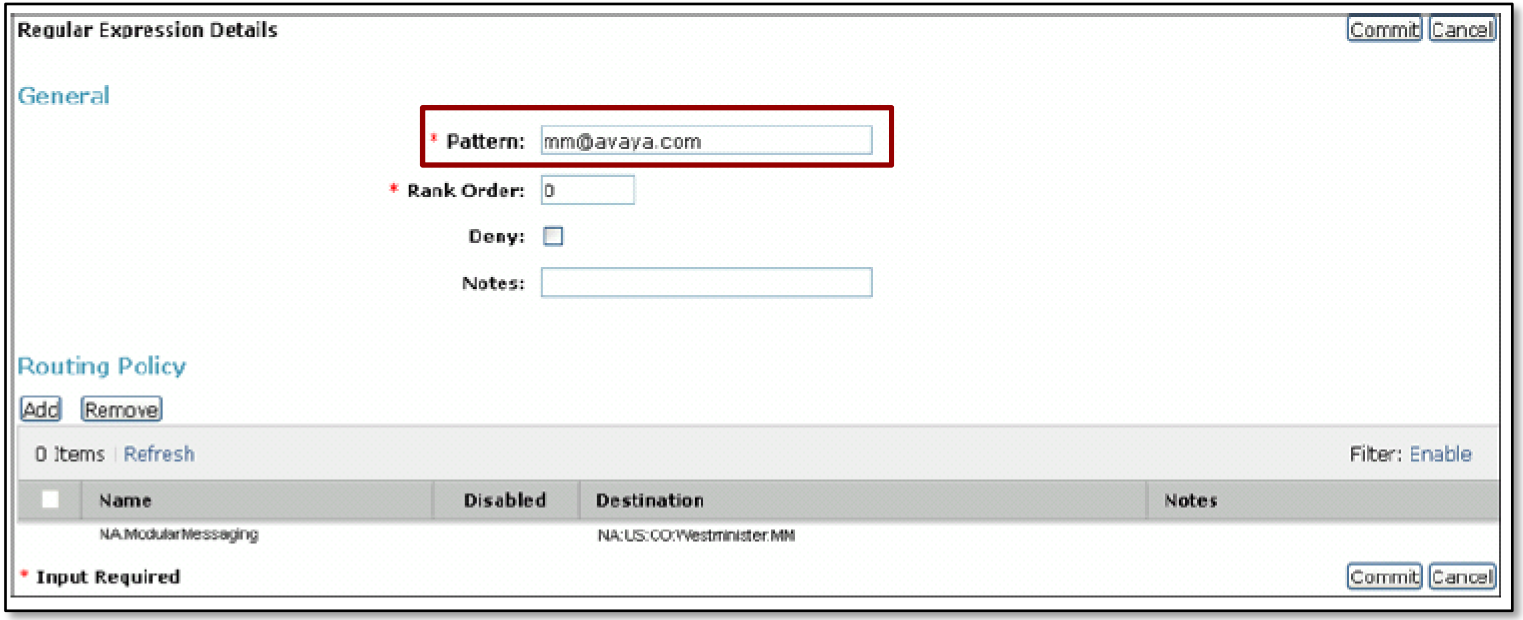
☐	Name	Disabled	Destination	Notes

SIP:12[5-9]{2}@sales\.net

Associates this Regular Expression to an existing Routing Policy

Regular Expressions and Modular Messaging

- Avaya SIP endpoints send a **SUBSCRIBE** message to CM to subscribe to a feature called **"message-summary"** which notifies them of messages waiting.
- When endpoints receive a MWI (Message Waiting Indication) from Modular Messaging, its SIP URI (mm@avaya.com) is used in the NOTIFY message back to the endpoints.
- A Regular Expression would have to be created for Session Manager to do a pattern match on Modular Messaging's SIP URI and properly route those messages to Modular Messaging and subscribers.
- A routing policy would also have to be created to route to a Modular Messaging SIP Entity.



Regular Expression Details

General

* Pattern:	mm@avaya.com
* Rank Order:	0
Deny:	□
Notes:	

Routing Policy

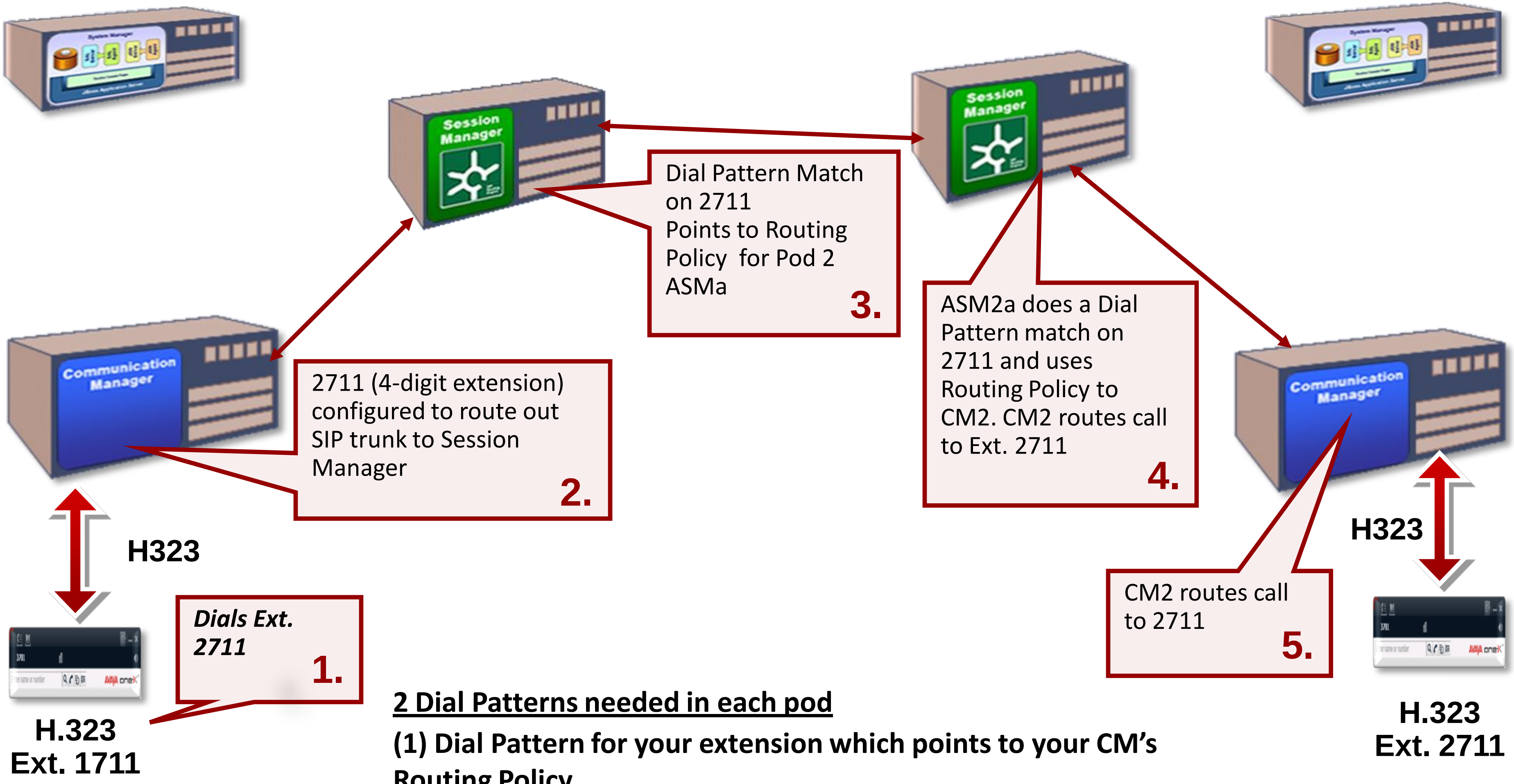
0 Items | Refresh

Filter: Enable

□	Name	Disabled	Destination	Notes
	NA.ModularMessaging		NA:US:CO:Westminister.MM	

* Input Required

Example Call Flow for H.323 to H.323 Routing



Dials Ext. 2711 **1.**

2711 (4-digit extension) configured to route out SIP trunk to Session Manager **2.**

Dial Pattern Match on 2711 Points to Routing Policy for Pod 2 ASMa **3.**

ASM2a does a Dial Pattern match on 2711 and uses Routing Policy to CM2. CM2 routes call to Ext. 2711 **4.**

CM2 routes call to 2711 **5.**

<u>2 Dial Patterns needed in each pod</u>

(1) Dial Pattern for your extension which points to your CM's Routing Policy

(1) Dial Pattern for your Pod Neighbor's extensions which point to Pod Neighbor's ASM Routing Policy

Exercise: Define Dial Pattern x7 to your CM

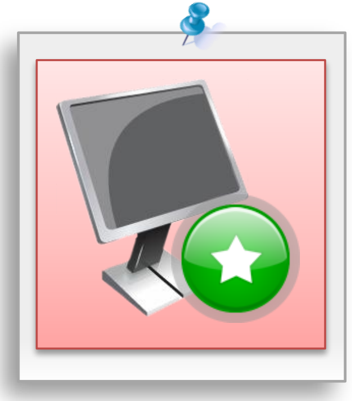
Objective: Create a Dial Pattern to route calls to your CMx.

This exercise requires shadowing to be setup between students as one student will complete the exercise and the other student shadows.

Step	Action
1	Select **Dial Patterns** from Routing Menu.
2	Select ***New*.**
3	Enter the dial pattern which is associated to each CM: Dial Pattern: x7 Min: 4 Max: 4 SIP Domain: -ALL-
4	Click **Add**
5	**Select** –Apply The Selected Routing Policies to All Originating Locations
6	**Select** Corresponding Routing Policy Dial Pattern x7, → RP to Your CMx
7	Click **Select.**
8	Select ***Commit*** to save your changes.

Exercise: Define Dial Pattern to Pod Neighbor's ASM

Objective: Create Dial Patterns to route calls between your ASM and your Pod neighbors' ASM's.

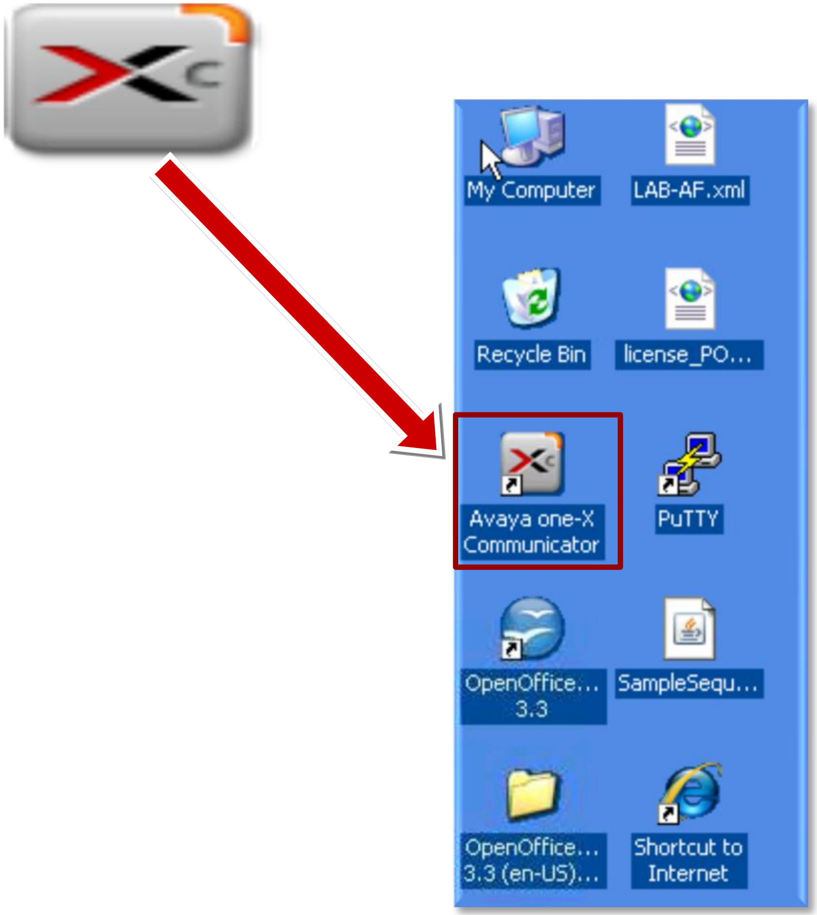


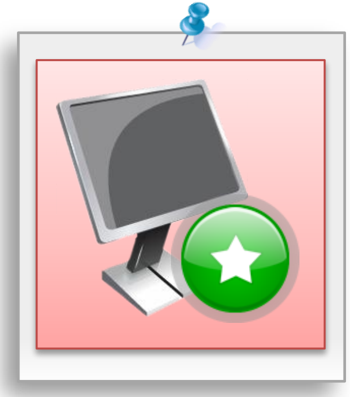
Step	Action
1	Select **Dial Patterns** from Routing Menu.
2	Select ***New*.**
3	Enter the dial pattern which is associated to each Pod Neighbor extension: **For example Pod1 can create Dial Pattern to Pod 2:** Dial Pattern: 27 Min: 4 Max: 4 SIP Domain: -ALL- **For Example Pod2 can create Dial Pattern to Pod1:** Dial Pattern: 17 Min: 4 Max: 4 SIP Domain: -ALL-
4	Click **Add**
5	**Select** –Apply The Selected Routing Policies to All Originating Locations
6	**Select** Corresponding Routing Policy Dial Patterns 17 → RP to ASM1 Dial Patterns 27 → RP to ASM2 Dial Patterns 37 → RP to ASM3 Dial Patterns 47 → RP to ASM4 Dial Patterns 57 → RP to ASM5 Dial Patterns 67 → RP to ASM6
7	Click **Select.**
8	Select ***Commit*** to save your changes.

Making Test Calls

Exercise: Access the One-X Communicator

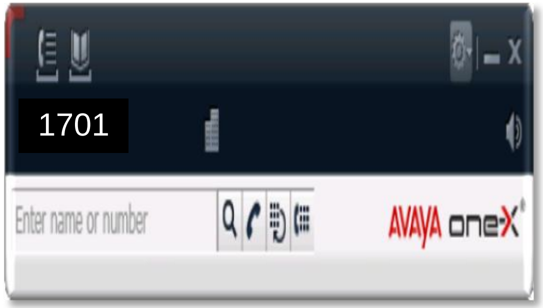
1. Double-click on the One-X Communicator shortcut on your desktop.



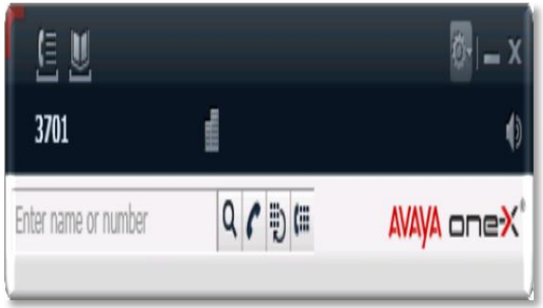


Exercise: Log into the H.323 One-X Communicator Phone

Step	Action
1	Log into your One-X Communicator softphone
2	Enter your extension and password, **123456**



SIP station – x711/x721



H323 station – x711/x721

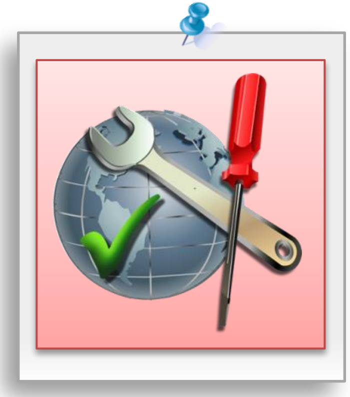
Student	Pod 1	Pod 2	Pod 3	Pod 4	Pod 5	Pod 6
Student a	1711	2711	3711	4711	5711	6711
Student b	1721	2721	3721	4721	5721	6721

Troubleshooting

Were you able to login successfully?

Yes!

No.



If not, do the following:

1. Retrace and validate your SIP Phone’s configuration.
2. Verify connectivity with systems

Exercise: Place an H.323 to H.323 call

This exercise will demonstrate routing by Session Manager from an H.323 endpoint to another H.323 endpoint registered to a CM.

Step	Action
1	From H.323 One-X Communicator dial your pod neighbor’s x711 or x721.

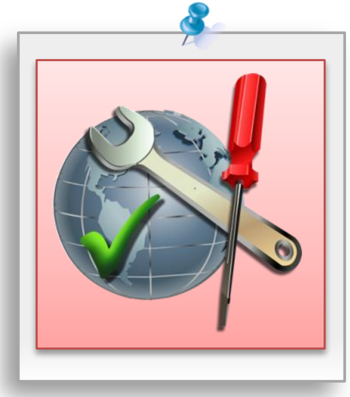
SIP station – x711/x721

H323 station – x711/x721

Student	Pod 1	Pod 2	Pod 3	Pod 4	Pod 5	Pod 6
Student a	1711	2711	3711	4711	5711	6711
Student b	1721	2721	3721	4721	5721	6721

Troubleshooting

Did the call complete successfully?



Yes!

No.

If not, do the following:

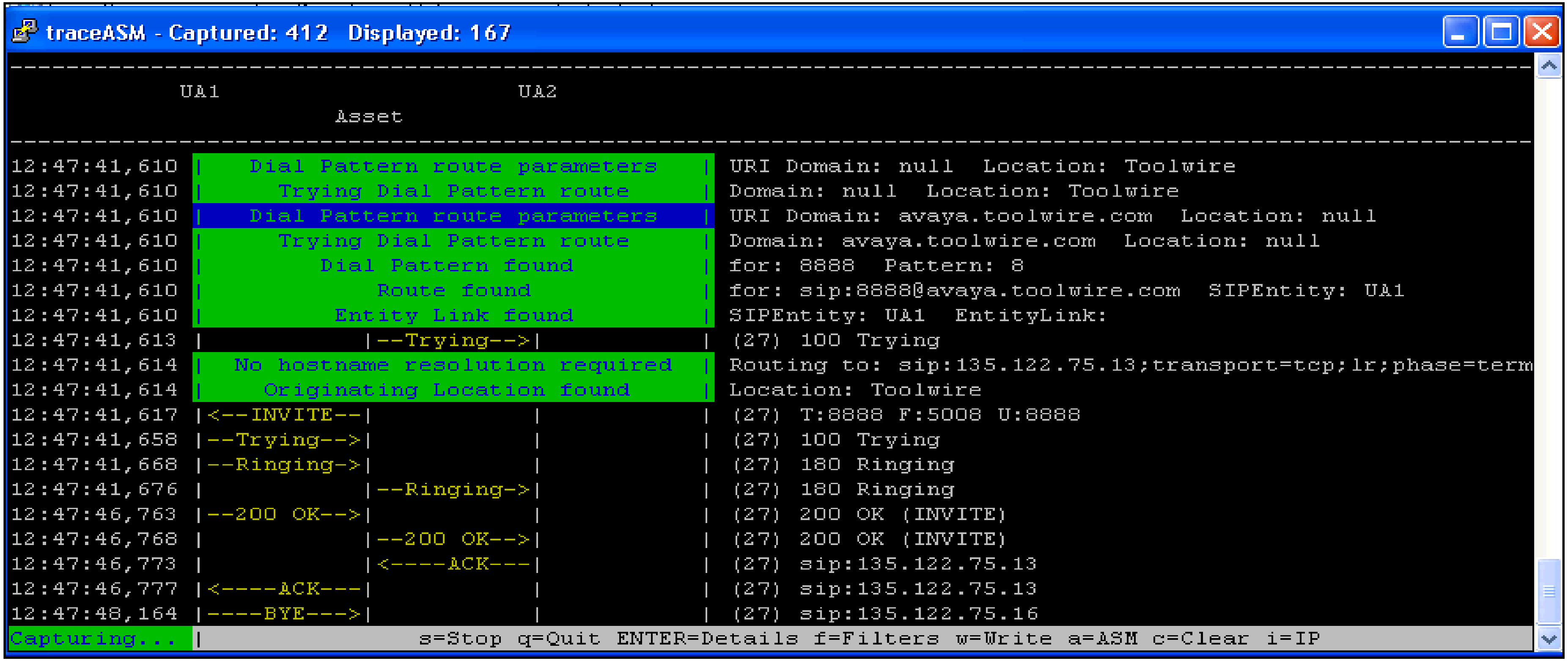
1. Retrace and validate your configuration
2. Run traceSM to diagnose the call flow and search for errors.

Tracing Calls

SIP Tracing

traceSM

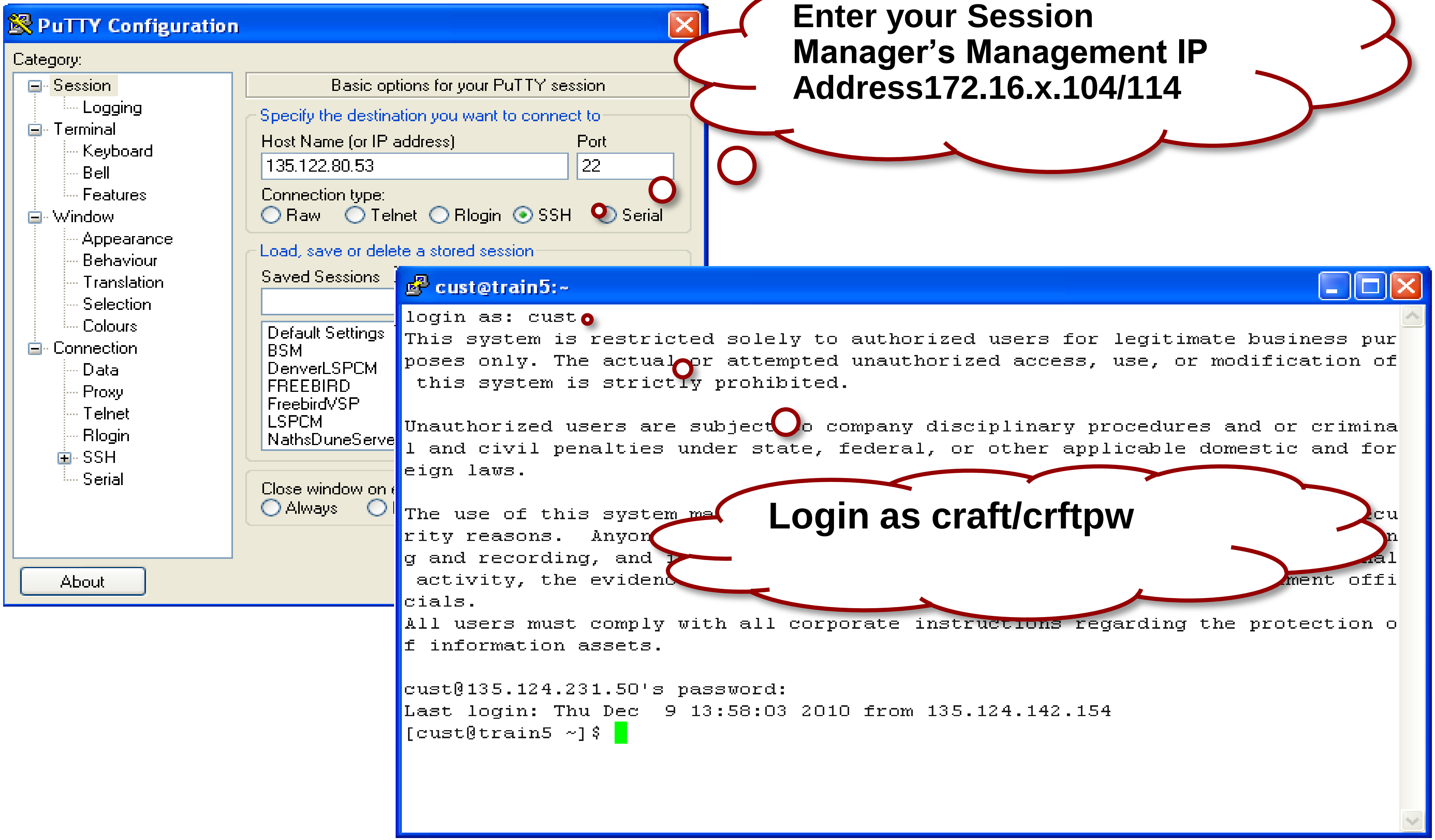
- Custom tool that allows us to trace SIP Requests & Responses in and out of the Session Manager. This tool enables us to more easily diagnose problems.



traceASM - Captured: 412 Displayed: 167

```
------------------------------------------------------------------------------------------------------------
            UA1                     UA2
                      Asset
------------------------------------------------------------------------------------------------------------
12:47:41,610 |    Dial Pattern route parameters   | URI Domain: null  Location: Toolwire
12:47:41,610 |      Trying Dial Pattern route     | Domain: null  Location: Toolwire
12:47:41,610 |    Dial Pattern route parameters   | URI Domain: avaya.toolwire.com  Location: null
12:47:41,610 |      Trying Dial Pattern route     | Domain: avaya.toolwire.com  Location: null
12:47:41,610 |         Dial Pattern found         | for: 8888  Pattern: 8
12:47:41,610 |             Route found            | for: sip:8888@avaya.toolwire.com  SIPEntity: UA1
12:47:41,610 |          Entity Link found         | SIPEntity: UA1  EntityLink:
12:47:41,613 |           |--Trying-->|            | (27) 100 Trying
12:47:41,614 |   No hostname resolution required  | Routing to: sip:135.122.75.13;transport=tcp;lr;phase=term
12:47:41,614 |    Originating Location found      | Location: Toolwire
12:47:41,617 |<--INVITE--|           |            | (27) T:8888 F:5008 U:8888
12:47:41,658 |--Trying-->|           |            | (27) 100 Trying
12:47:41,668 |--Ringing->|           |            | (27) 180 Ringing
12:47:41,676 |           |--Ringing->|            | (27) 180 Ringing
12:47:46,763 |--200 OK-->|           |            | (27) 200 OK (INVITE)
12:47:46,768 |           |--200 OK-->|            | (27) 200 OK (INVITE)
12:47:46,773 |           |<-----ACK---|           | (27) sip:135.122.75.13
12:47:46,777 |<-----ACK---|          |            | (27) sip:135.122.75.13
12:47:48,164 |----BYE--->|           |            | (27) sip:135.122.75.16
Capturing... |           s=Stop q=Quit ENTER=Details f=Filters w=Write a=ASM c=Clear i=IP
```

Accessing the Session Manager Host



Specify the destination you want to connect to

Host Name (or IP address): 135.122.80.53

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

```
login as: cust
This system is restricted solely to authorized users for legitimate business pur
poses only. The actual or attempted unauthorized access, use, or modification of
 this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or crimina
l and civil penalties under state, federal, or other applicable domestic and for
eign laws.

The use of this system ma                                                    cu
rity reasons.  Anyon                                                          n
g and recording, and i                                                       al
 activity, the evidenc                                               ment offi
cials.
All users must comply with all corporate instructions regarding the protection o
f information assets.

cust@135.124.231.50's password:
Last login: Thu Dec  9 13:58:03 2010 from 135.124.142.154
[cust@train5 ~]$
```

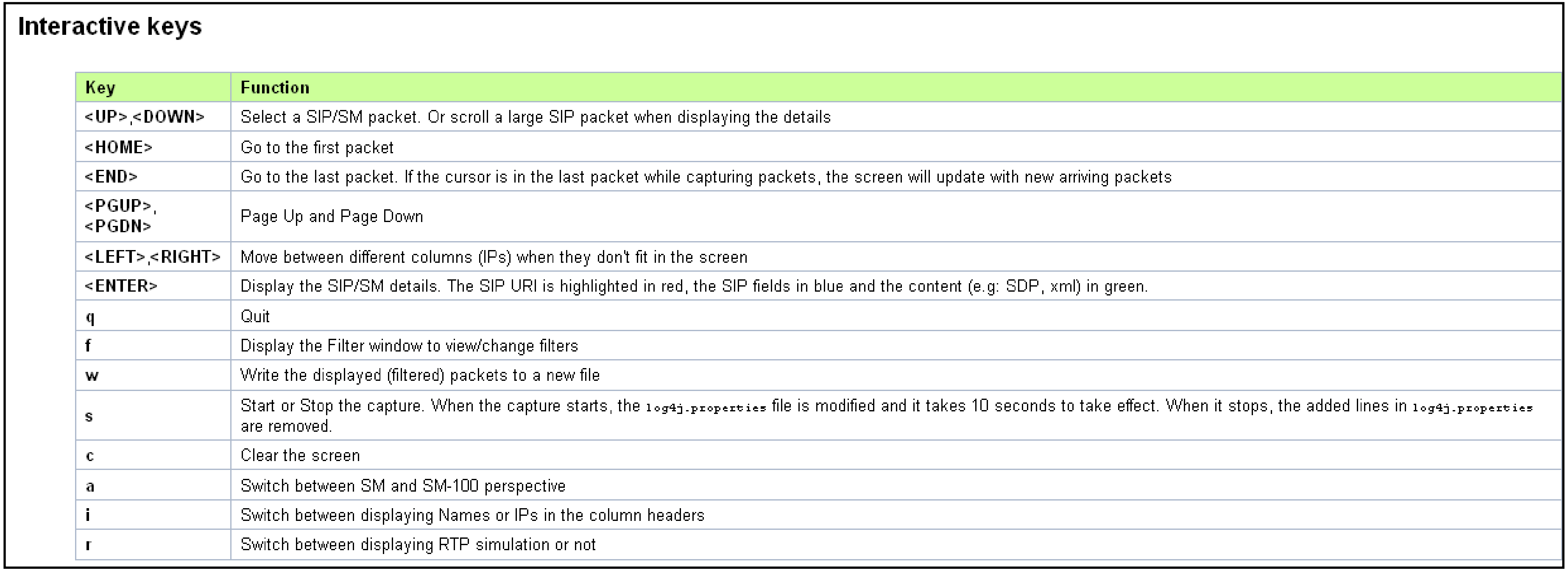
Enter your Session Manager's Management IP Address172.16.x.104/114

Login as craft/crftpw

SIP Tracing

traceSM

- Type ***traceSM -h*** at the command line to get help with the different arguments that the script supports.



Interactive keys

Key	Function
<UP>,<DOWN>	Select a SIP/SM packet. Or scroll a large SIP packet when displaying the details
<HOME>	Go to the first packet
<END>	Go to the last packet. If the cursor is in the last packet while capturing packets, the screen will update with new arriving packets
<PGUP>, <PGDN>	Page Up and Page Down
<LEFT>,<RIGHT>	Move between different columns (IPs) when they don't fit in the screen
<ENTER>	Display the SIP/SM details. The SIP URI is highlighted in red, the SIP fields in blue and the content (e.g: SDP, xml) in green.
q	Quit
f	Display the Filter window to view/change filters
w	Write the displayed (filtered) packets to a new file
s	Start or Stop the capture. When the capture starts, the `log4j.properties` file is modified and it takes 10 seconds to take effect. When it stops, the added lines in `log4j.properties` are removed.
c	Clear the screen
a	Switch between SM and SM-100 perspective
i	Switch between displaying Names or IPs in the column headers
r	Switch between displaying RTP simulation or not

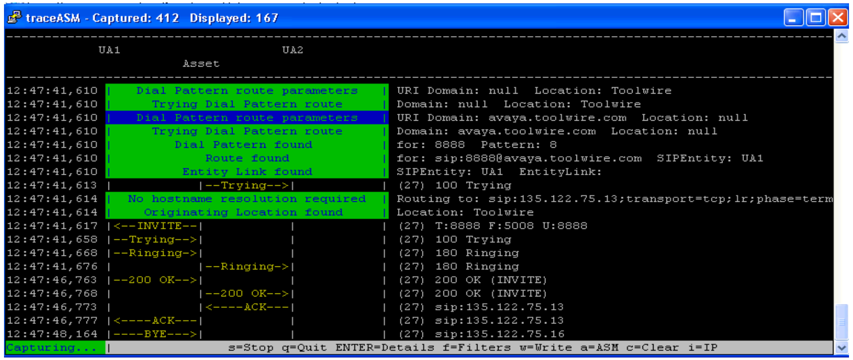
Exercise: Run traceSM

Step	Action
1	SSH into the Session Manager host **172.16.x.104** or **.114** Login **craft** password: **crftpw** and then execute:
2	**traceSM –x**
3	‘s’ to start the capture

Place the previous call again

Look for:

- Dial Pattern matches and Routing Policy selection
- Examine SIP messages between CM and ASM



traceASM - Captured: 412 Displayed: 167

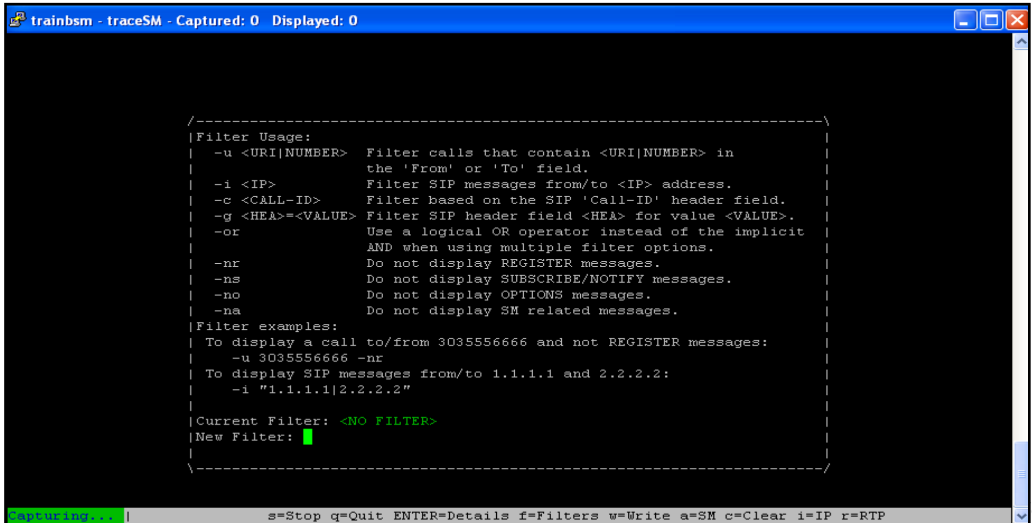
```
-----------------------------------------------------------------------------------------------------------
             UA1                         UA2
                         Asset
-----------------------------------------------------------------------------------------------------------
12:47:41,610 |     Dial Pattern route parameters     | URI Domain: null  Location: Toolwire
12:47:41,610 |       Trying Dial Pattern route       | Domain: null  Location: Toolwire
12:47:41,610 |     Dial Pattern route parameters     | URI Domain: avaya.toolwire.com  Location: null
12:47:41,610 |       Trying Dial Pattern route       | Domain: avaya.toolwire.com  Location: null
12:47:41,610 |          Dial Pattern found           | for: 8888  Pattern: 8
12:47:41,610 |              Route found              | for: sip:8888@avaya.toolwire.com  SIPEntity: UA1
12:47:41,610 |           Entity Link found           | SIPEntity: UA1  EntityLink:
12:47:41,613 |            |--Trying-->|             | (27) 100 Trying
12:47:41,614 |    No hostname resolution required    | Routing to: sip:135.122.75.13;transport=tcp;lr;phase=term
12:47:41,614 |      Originating Location found       | Location: Toolwire
12:47:41,617 |<--INVITE--|            |             | (27) T:8888 F:5008 U:8888
12:47:41,658 |--Trying-->|            |             | (27) 100 Trying
12:47:41,668 |--Ringing->|            |             | (27) 180 Ringing
12:47:41,676 |           |--Ringing->|             | (27) 180 Ringing
12:47:46,763 |--200 OK-->|            |             | (27) 200 OK (INVITE)
12:47:46,768 |           |--200 OK-->|             | (27) 200 OK (INVITE)
12:47:46,773 |           |<----ACK---|             | (27) sip:135.122.75.13
12:47:46,777 |<----ACK---|            |             | (27) sip:135.122.75.13
12:47:48,164 |----BYE--->|            |             | (27) sip:135.122.75.16
Capturing... |               s=Stop q=Quit ENTER=Details f=Filters w=Write a=ASM c=Clear i=IP
```

TraceSM is delivered under /opt/Avaya/contrib/bin

SIP Tracing

traceSM

- Once traceSM is running, type ‘F’ to apply a filter.
- Examples
  - -no = no OPTIONS
  - -nr = no REGISTERS
  - -ns = no SUBSCRIBES
  - -u 1901 will filter calls that contain that URI in the from or to headers
  - You can apply multple filters:
    - **-u 1901 –no –ns –nr**
      - The above will show only messages to/from 1901 and hide OPTIONS, SUBSCRIBES and REGISTERS

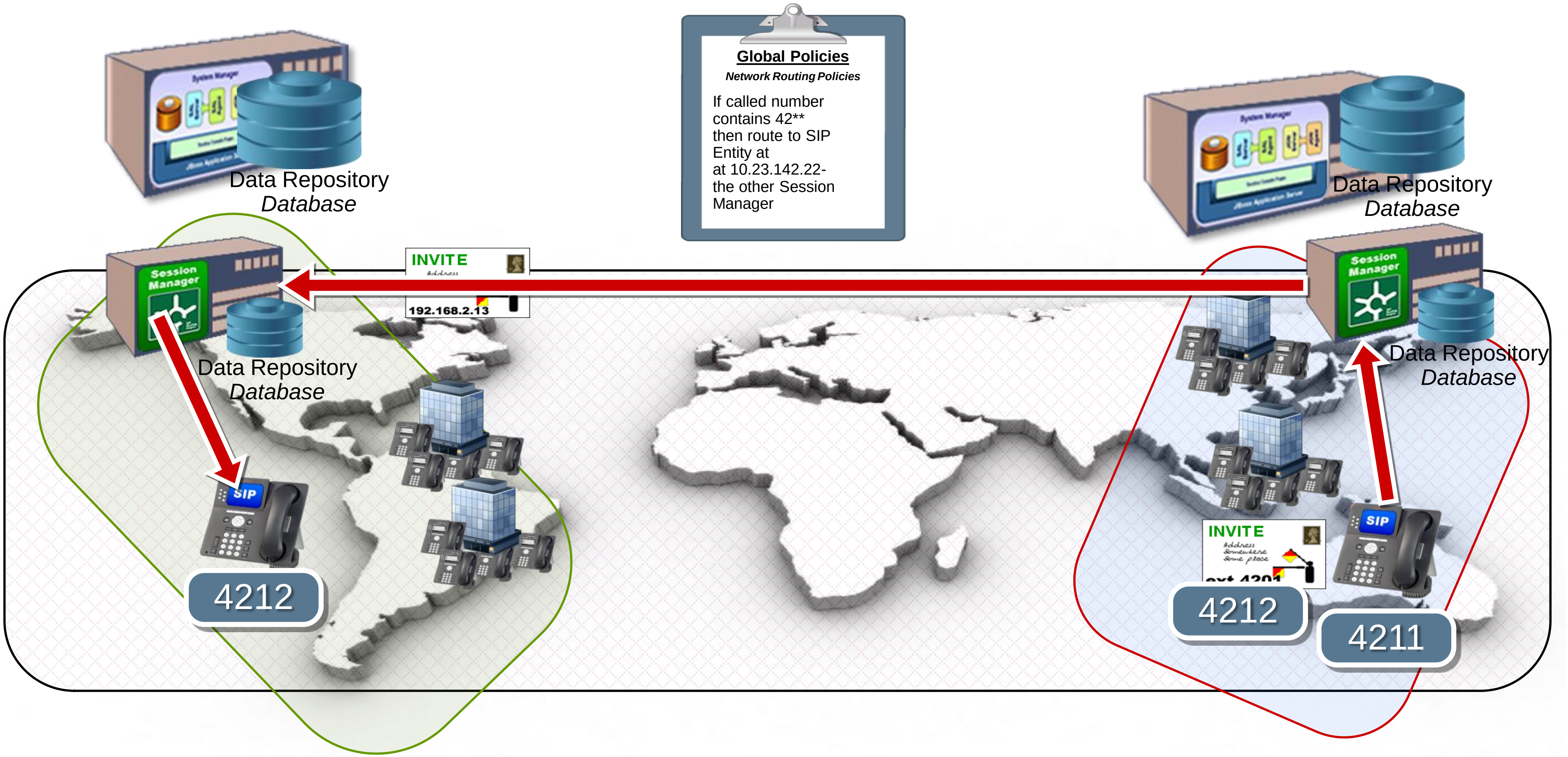


```
/-----------------------------------------------------------------------\
|Filter Usage:                                                          |
|   -u <URI|NUMBER>  Filter calls that contain <URI|NUMBER> in          |
|                    the 'From' or 'To' field.                          |
|   -i <IP>          Filter SIP messages from/to <IP> address.          |
|   -c <CALL-ID>     Filter based on the SIP 'Call-ID' header field.    |
|   -g <HEA>=<VALUE> Filter SIP header field <HEA> for value <VALUE>.   |
|   -or              Use a logical OR operator instead of the implicit  |
|                    AND when using multiple filter options.            |
|   -nr              Do not display REGISTER messages.                  |
|   -ns              Do not display SUBSCRIBE/NOTIFY messages.          |
|   -no              Do not display OPTIONS messages.                   |
|   -na              Do not display SM related messages.                |
|Filter examples:                                                       |
| To display a call to/from 3035556666 and not REGISTER messages:       |
|    -u 3035556666 -nr                                                  |
| To display SIP messages from/to 1.1.1.1 and 2.2.2.2:                  |
|    -i "1.1.1.1|2.2.2.2"                                               |
|                                                                       |
|Current Filter: <NO FILTER>                                            |
|New Filter:                                                            |
|                                                                       |
\-----------------------------------------------------------------------/

Capturing... |           s=Stop q=Quit ENTER=Details f=Filters w=Write a=SM c=Clear i=IP r=RTP
```

AVAYA | LEARNING

SIP to SIP Routing Using Routing Policies

SIP to SIP Routing with Multiple Session Managers



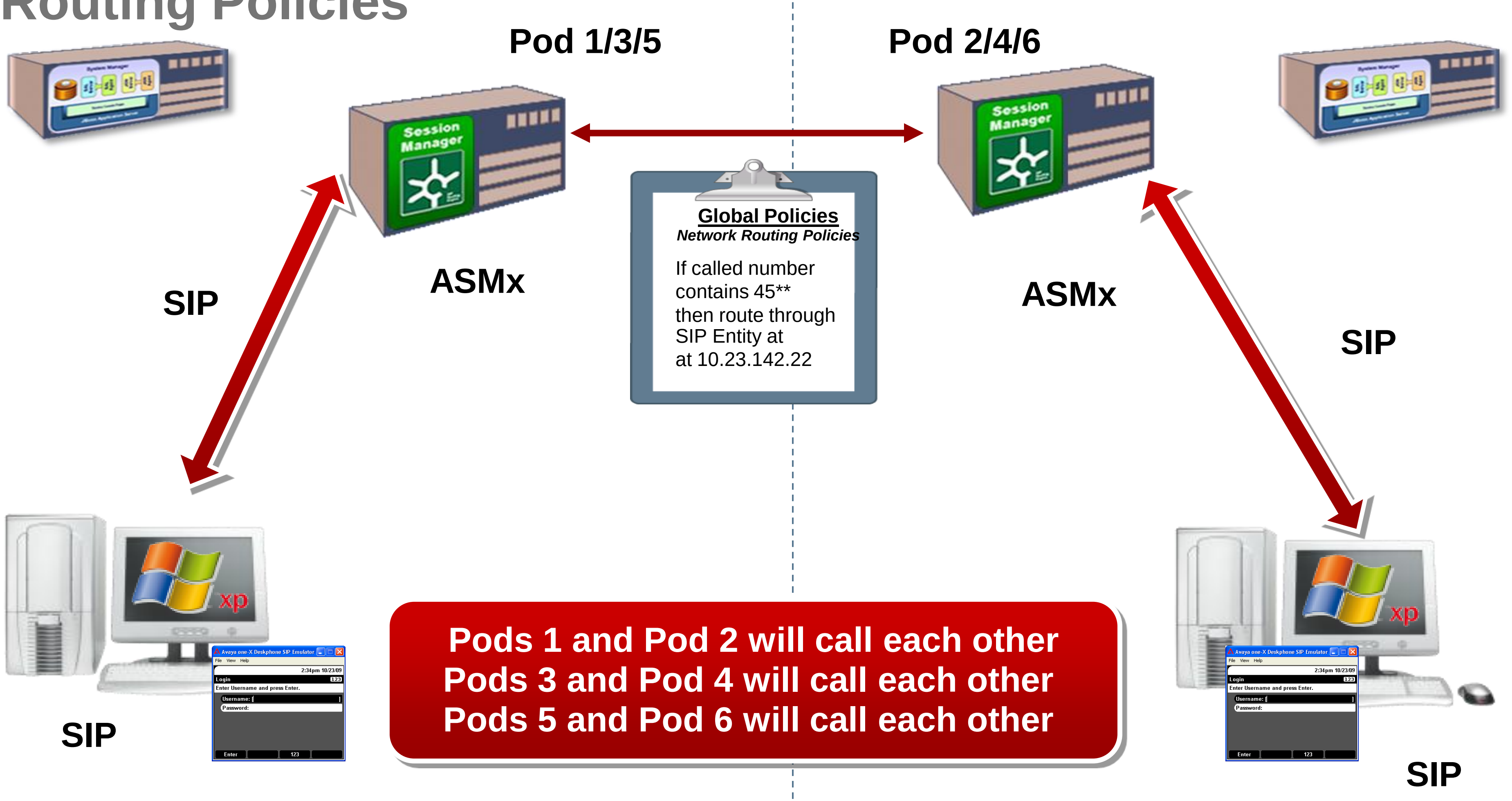
Global Policies

Network Routing Policies

If called number contains 42** then route to SIP Entity at at 10.23.142.22- the other Session Manager

- Routing policies are also used when SIP endpoints are managed in different Session Manager and are not part of the same cluster.

Routing Scenario 2: SIP to SIP Call Routing Using Routing Policies



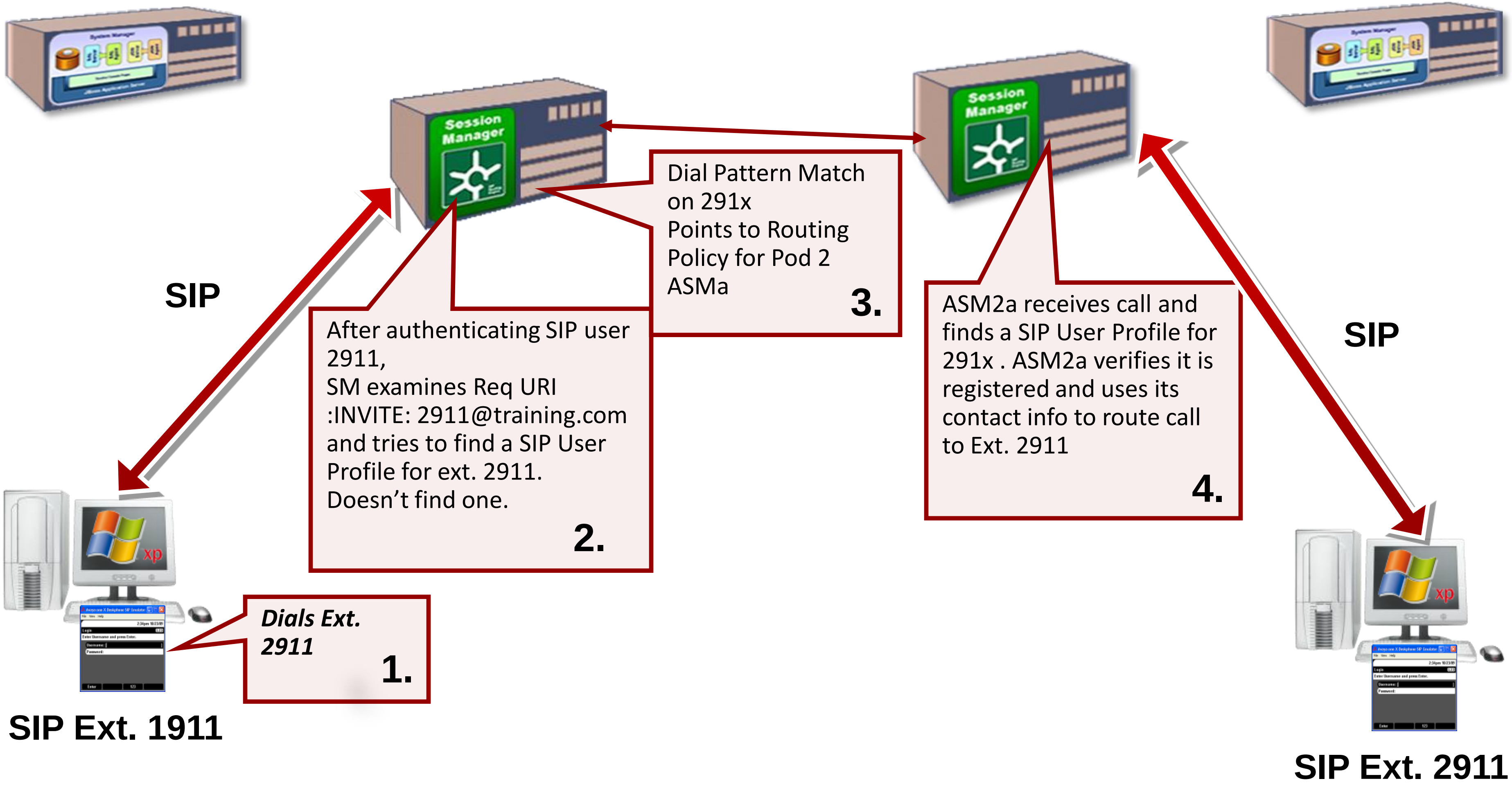
Global Policies

Network Routing Policies

If called number contains 45** then route through SIP Entity at at 10.23.142.22

Pods 1 and Pod 2 will call each other
Pods 3 and Pod 4 will call each other
Pods 5 and Pod 6 will call each other

Example Call Flow for SIP to SIP with Routing Policies



Dials Ext. 2911

1.

After authenticating SIP user 2911,
SM examines Req URI
:INVITE: 2911@training.com
and tries to find a SIP User Profile for ext. 2911.
Doesn’t find one.

2.

Dial Pattern Match
on 291x
Points to Routing
Policy for Pod 2
ASMa

3.

ASM2a receives call and finds a SIP User Profile for 291x . ASM2a verifies it is registered and uses its contact info to route call to Ext. 2911

4.

SIP Ext. 1911

SIP Ext. 2911

Prep for Next Call Routing Scenario: SIP-to-SIP Calling using NRP

What elements need to be configured in order for calls to get routed successfully?

Once all of the elements have been configured, each Session Manager will be able to route SIP calls to the other Session Manager in the neighboring Pod.

What needs to be done first?

1. ?
2. ?
3. ?
4. ?

Make a Call

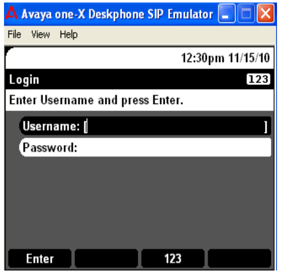
Exercise: Test SIP to SIP Routing using NRP

Objective: This exercise will test SIP-to-SIP routing by Session Manager using Routing Policies.

Step	Action
1	From your **x911** / **x921** SIP extension, dial your partner's **x911**/ **x921** extension

172.16.x.105

SIP station – x911/x921



Avaya one-X Deskphone SIP Emulator

File View Help

12:30pm 11/15/10

Login 123

Enter Username and press Enter.

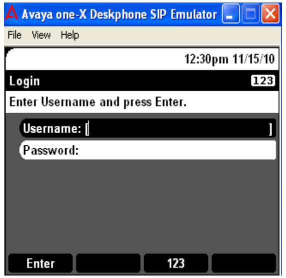
Username: [ ]

Password:

Enter 123

172.16.x.105

SIP station – x911/x921



Avaya one-X Deskphone SIP Emulator

File View Help

12:30pm 11/15/10

Login 123

Enter Username and press Enter.

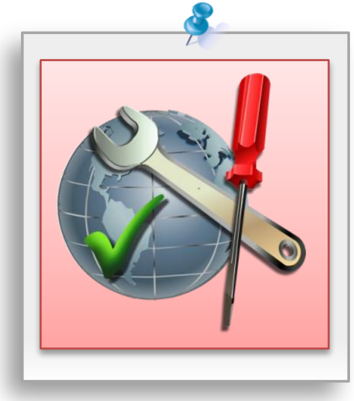
Username: [ ]

Password:

Enter 123

Troubleshooting

Did the call complete successfully?



Yes!

No.

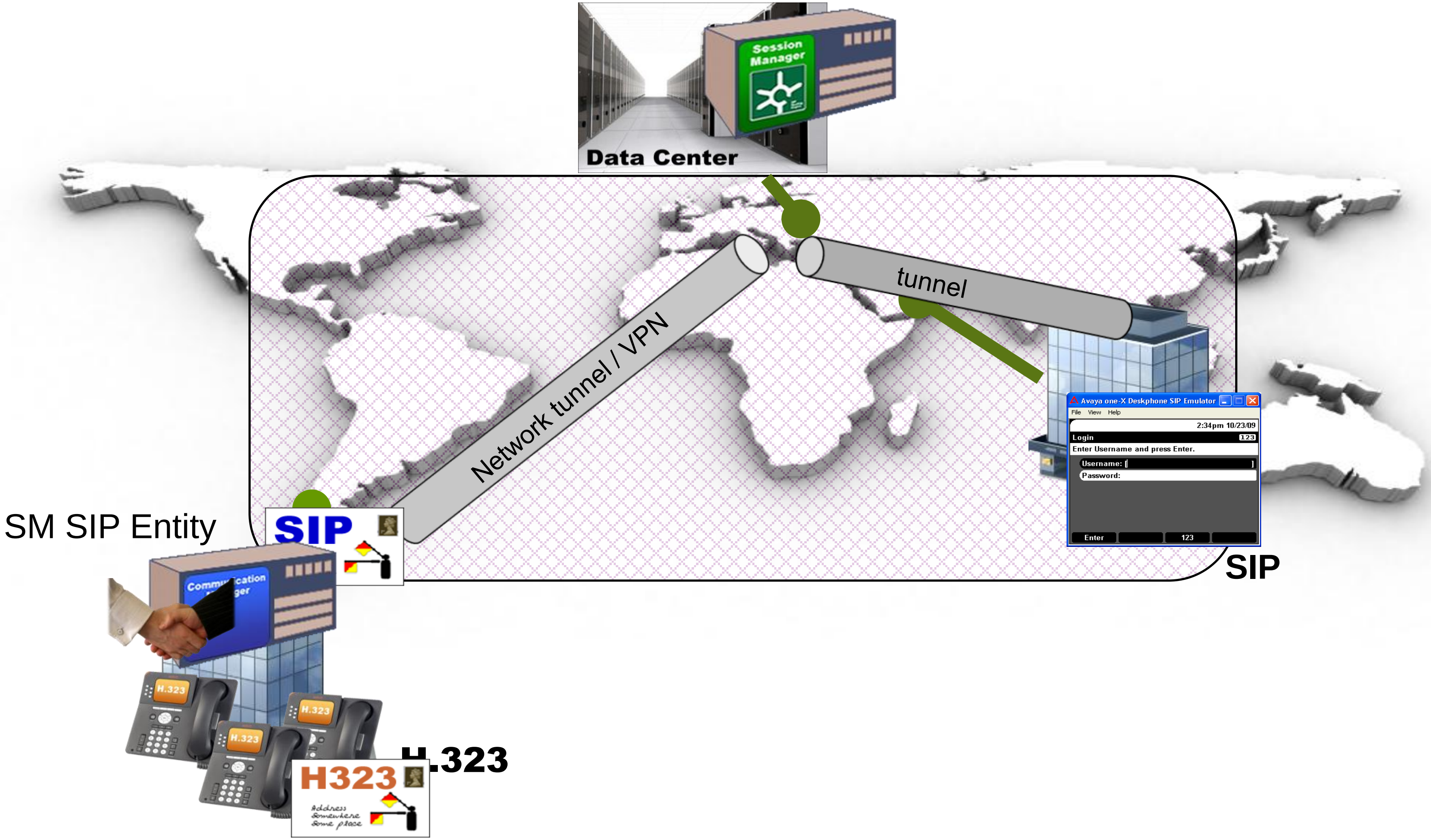
If not, do the following:

- Retrace and validate your configuration.
- Run traceSM to diagnose the call flow and search for errors.

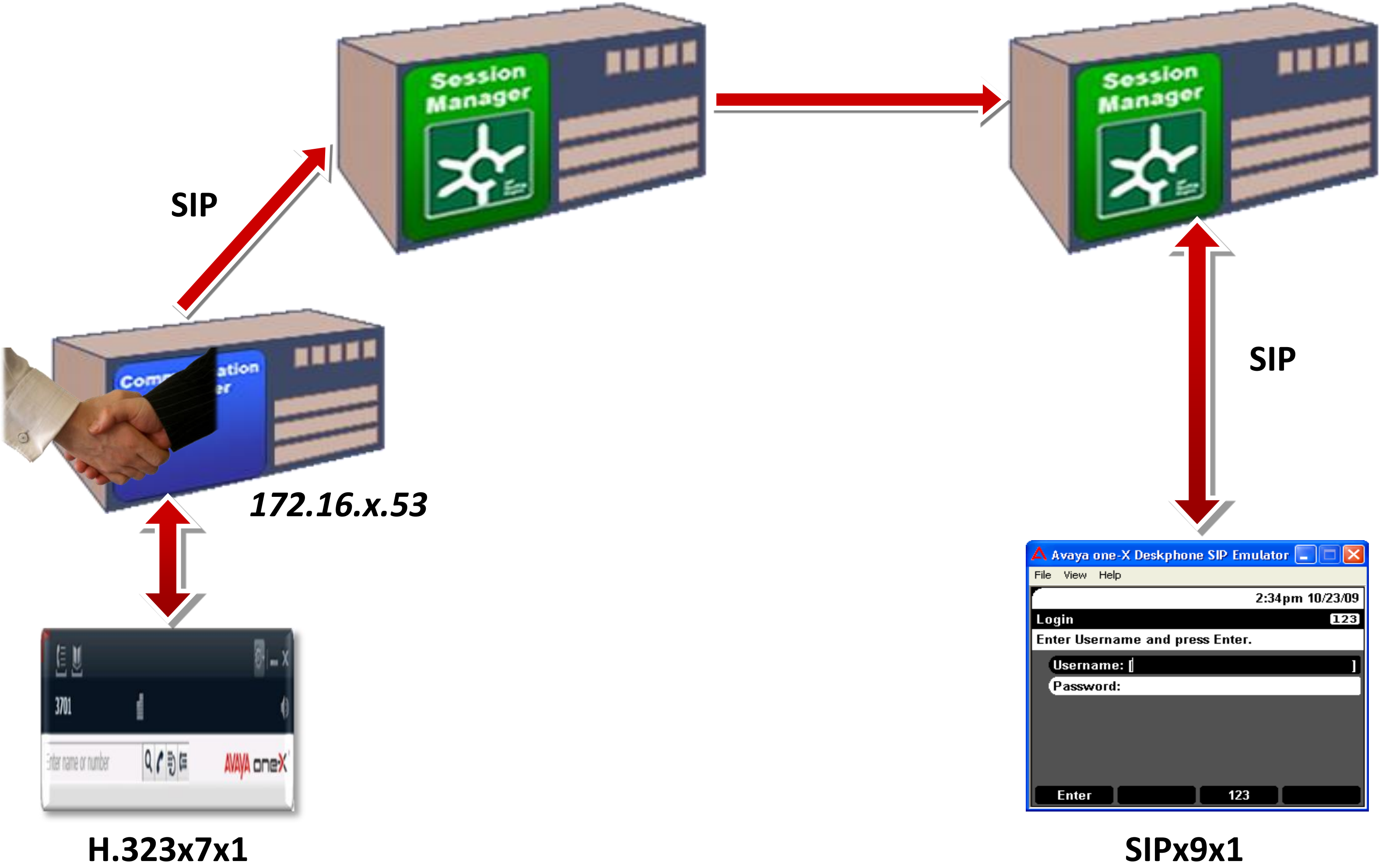
AVAYA | LEARNING

H323 to SIP Routing

Session Manager & Communication Manager



Prepare to Place a Call from an H323 Phone to SIP User



Avaya one-X Deskphone SIP Emulator

File View Help

2:34pm 10/23/09

Login 123

Enter Username and press Enter.

Username: [ ]

Password:

Enter 123

Prep

What additional configuration is required for this call to complete successfully?

Assume the SIP Domain and Location are configured.

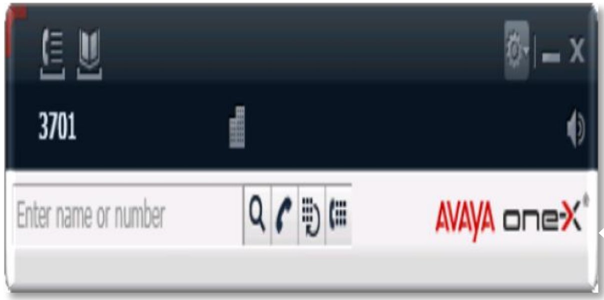
Does your Session Manager:

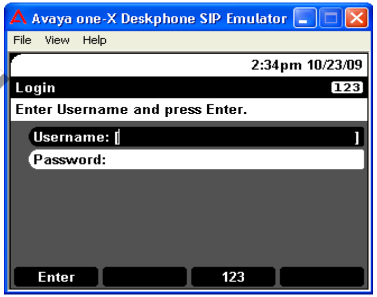
- Recognize the CM as a SIP Entity?
- Know how to communicate with CM?
- Recognize the registered SIP User?

Exercise: Place a call from H.323 User to SIP User

Step	Action
1	Log into your **x7x1** H.323 Station
2	Log into your **x9x1** SIP Phone
3	Place the call

SIP	Pod 1	Pod 2	Pod 3	Pod 4	Pod 5	Pod 6
Student a	1911	2911	3911	4911	5911	6911
Student b	1921	2921	3921	4921	5921	6921





2:34pm 10/23/09

Login 123

Enter Username and press Enter.

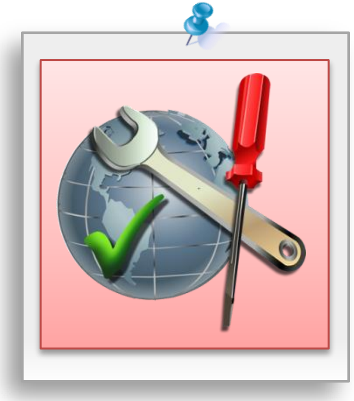
Username: [ ]

Password:

H.323	Pod 1	Pod 2	Pod 3	Pod 4	Pod 5	Pod 6
Student a	1711	2711	3711	4711	5711	6711
Student b	1721	2721	3721	4721	5721	6721

Troubleshooting

Did the call complete successfully?



Yes!

No.

If not, do the following:

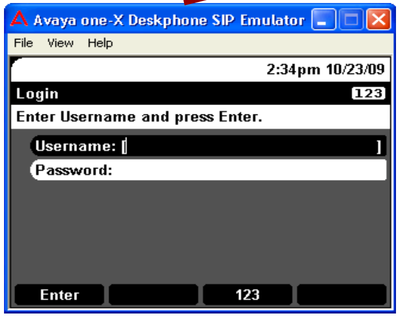
1. Retrace and validate your configuration.
2. Run traceSM to diagnose the call flow and search for errors.

AVAYA | LEARNING

SIP to H323 calls

Place a Call from a SIP Phone to H.323 Phone

SIP



Avaya one-X Deskphone SIP Emulator

File View Help

2:34pm 10/23/09

Login 123

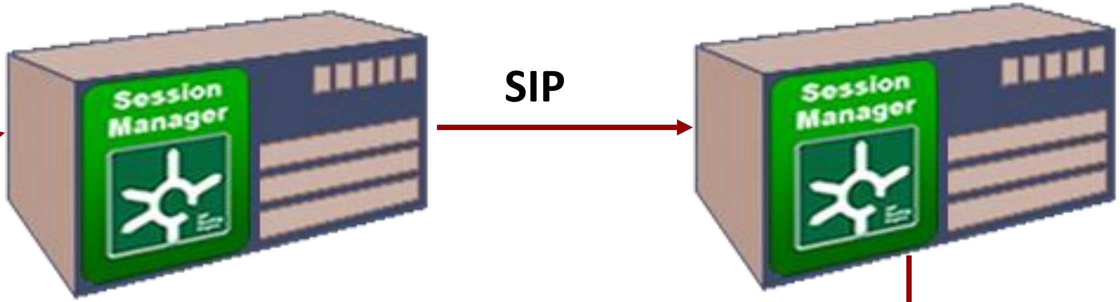
Enter Username and press Enter.

Username: [ ]

Password:

Enter | | 123 |

SIP
SIP:x9x1@training.com



Communication Manager

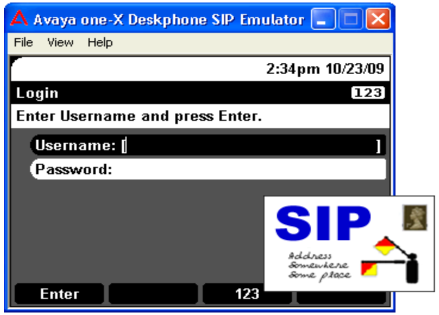
172.16.x.53

H.323
x7x1@training.com

What additional configuration do we need to make to place this call?

- Assume the SIP Domain and Location are configured.
- Does your Session Manager:
  - Recognize the CM as a SIP Entity?
  - Know how to communicate with CM?
  - Recognize the registered SIP User?

Exercise: SIP to H.323 Calling

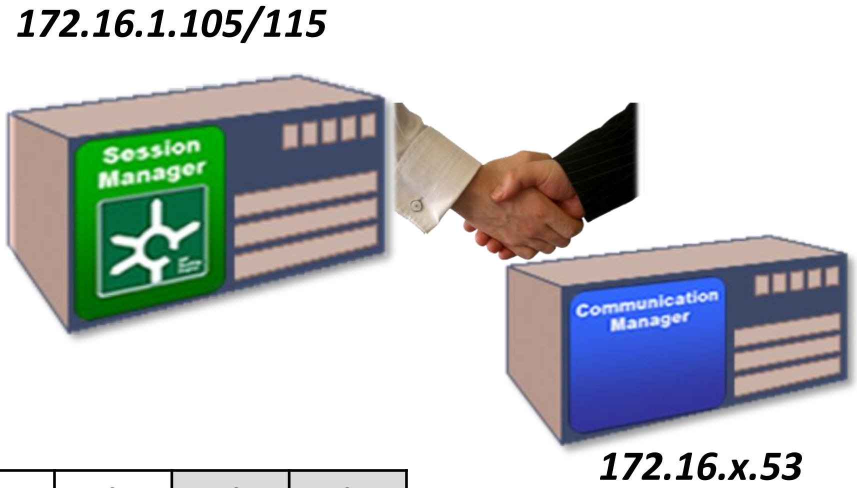


2:34pm 10/23/09

Enter Username and press Enter.

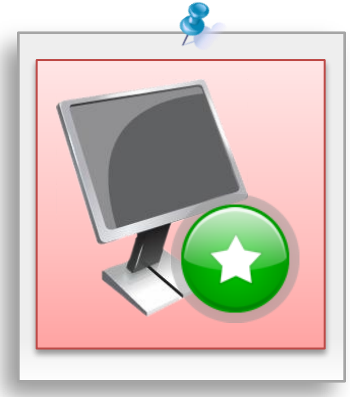
Username: [

Password:

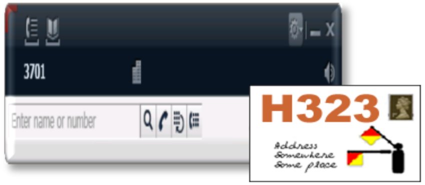


172.16.1.105/115

172.16.x.53



SIP	Pod 1	Pod 2	Pod 3	Pod 4	Pod 5	Pod 6
Student a	1911	2911	3911	4911	5911	6911
Student b	1921	2921	3921	4921	5921	6921



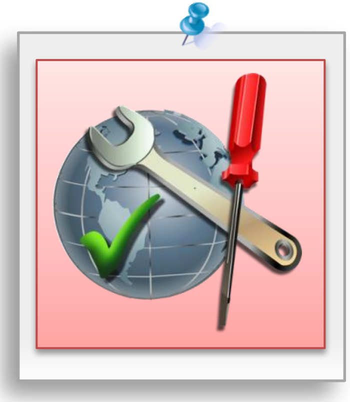
H.323	Pod 1	Pod 2	Pod 3	Pod 4	Pod 5	Pod 6
Student a	1711	2711	3711	4711	5711	6711
Student b	1721	2721	3721	4721	5721	6721

Troubleshooting

Did the call complete successfully?

Yes!

No.



If not, do the following:

1. Retrace and validate your configuration.
2. Run traceSM to diagnose the call flow and search for errors.

Questions and Answers

Lesson Summary

You have completed the following lesson objectives:

- Review and configure the following to support centralized call routing within the enterprise:
  - Domain
  - Location
  - SIP Entities
  - Entity Links
  - Time Ranges
  - Routing Policies
  - Dial Patterns
  - Regular Expressions

Lesson 6

Integration and Adaptation

Lesson Objective

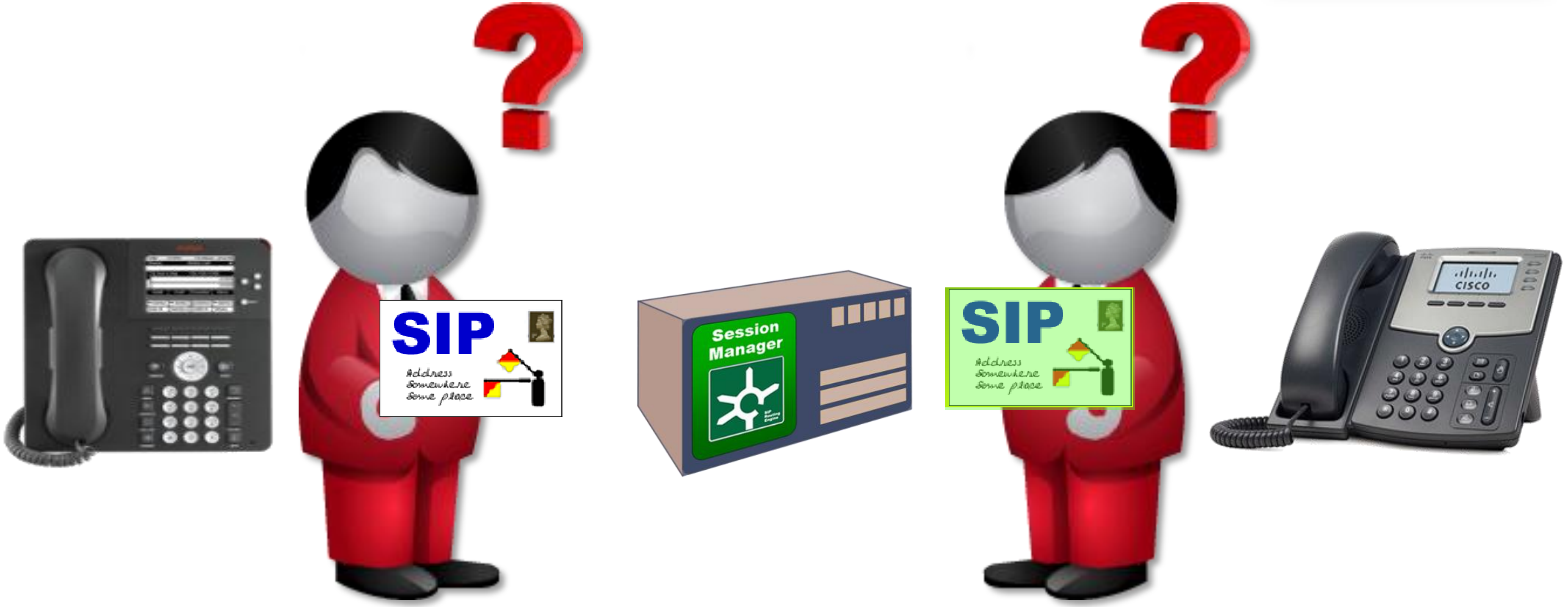
After completing this lesson, you will be able to:

- Manipulate SIP message content and dialed digits through the use of Adaptation modules.

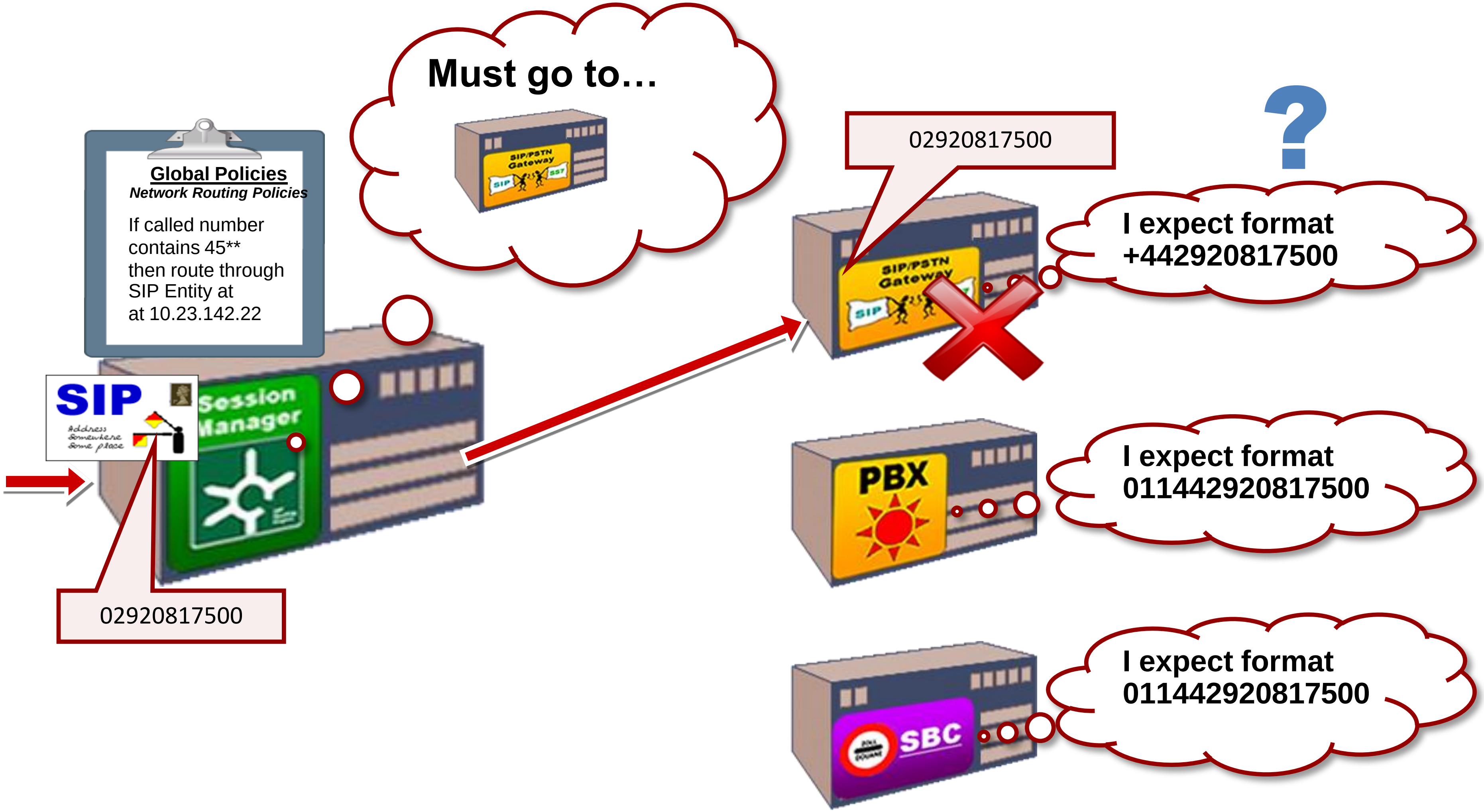
Integration and Adaptation

What can be modified so that SIP messages from different vendors can be processed?

- Dialled Number Format
- Domain
- SIP Message Format



Number Adaptation



Must go to…

Global Policies

Network Routing Policies

If called number contains 45** then route through SIP Entity at at 10.23.142.22

02920817500

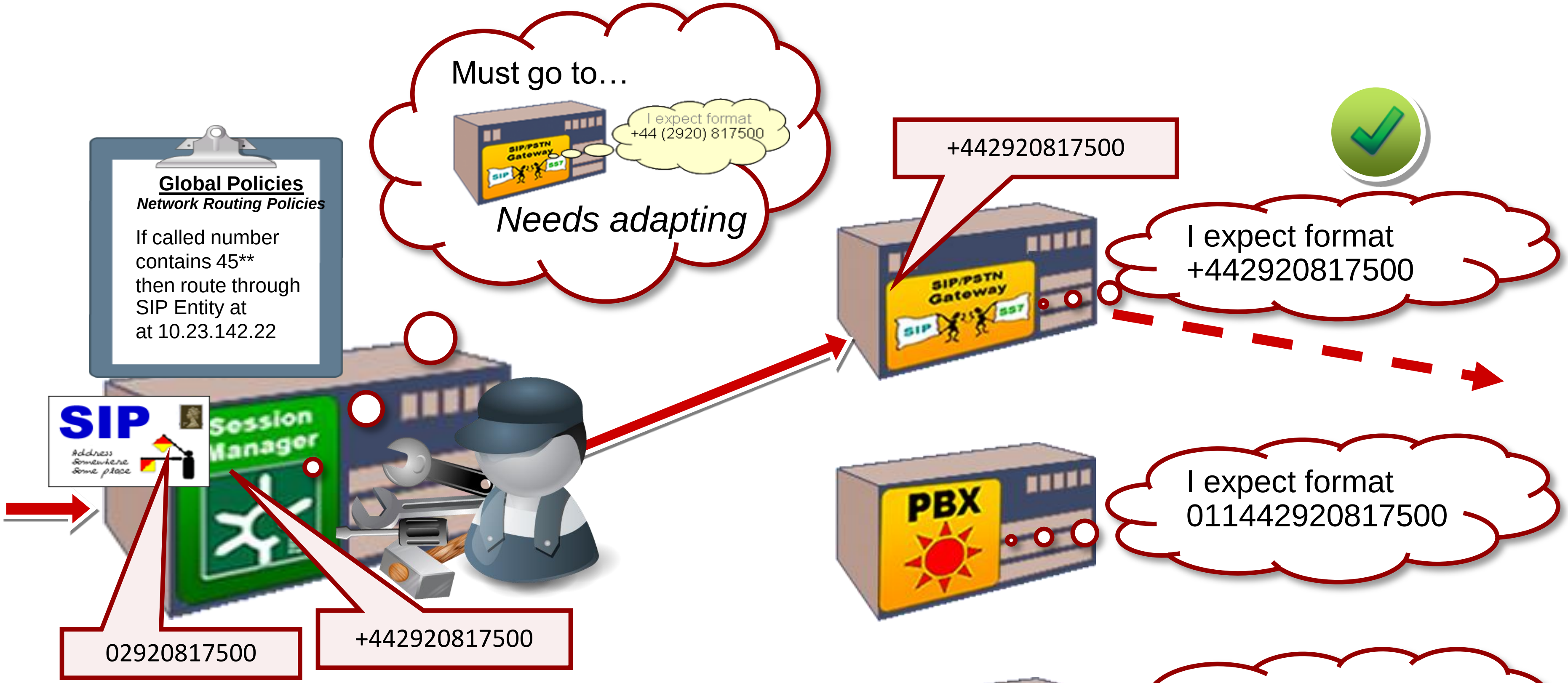
02920817500

I expect format +442920817500

I expect format 011442920817500

I expect format 011442920817500

Number Adaptation (continued)



Must go to…
SIP/PSTN Gateway
SIP
SS7
I expect format +44 (2920) 817500
Needs adapting
Global Policies
Network Routing Policies
If called number contains 45** then route through SIP Entity at at 10.23.142.22
SIP
Address Somewhere Some place
Session Manager
02920817500
+442920817500
+442920817500
SIP/PSTN Gateway
SIP
SS7
I expect format +442920817500
PBX
I expect format 011442920817500
SBC
I expect format 011442920817500

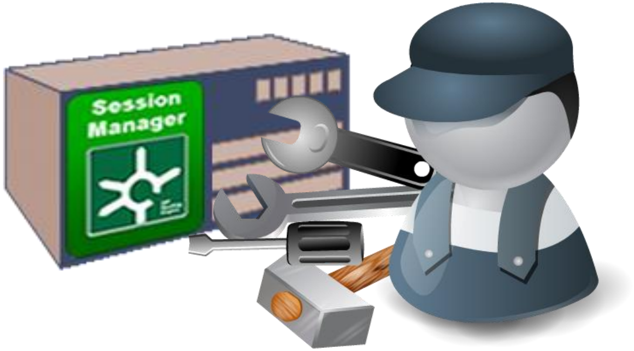
Note

Customers should check the support.avaya.com website for interoperability testing with their system prior to implementation.

Adaptation Modules

Session Manager uses Adaptation Modules to create adaptations, for example: DigitConversionAdapter

- Adaptation direction
- Matching digit pattern and corresponding digits to remove/insert
- Domain name change for source components and destination components
- Replace hostnames in the Request URI
- Modify origination headers such as: From, PAI, History Info
- Modify destination type headers such as: Request URI, Contact,To, Message Account and Refer-to



Adaptation Modules (continued)

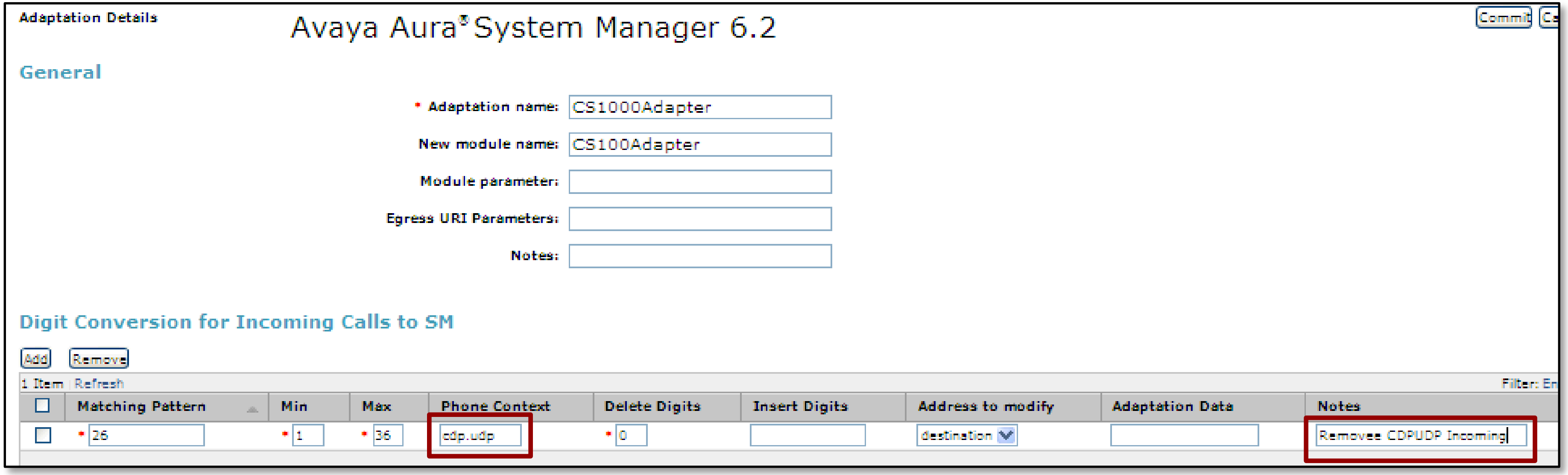
Additional extensions are delivered to support additional service providers:

- VerizonAdapter
- AttAdapter
- CiscoAdapter
- OrangeAdapter
- CS1000Adapter
- ModularMessagingAdapter
- DiversionTypeAdapter
- SkypeAdapter

Refer to the ***Administering Session Manager 6.2*** on the support.avaya.com website.

CS1000 Adapter

The CS 1000 Adapter is designed to translate CS 1000 SIP URI phone-context messages sent between the CS 1000 SIP Gateway and the Session Manager.



General

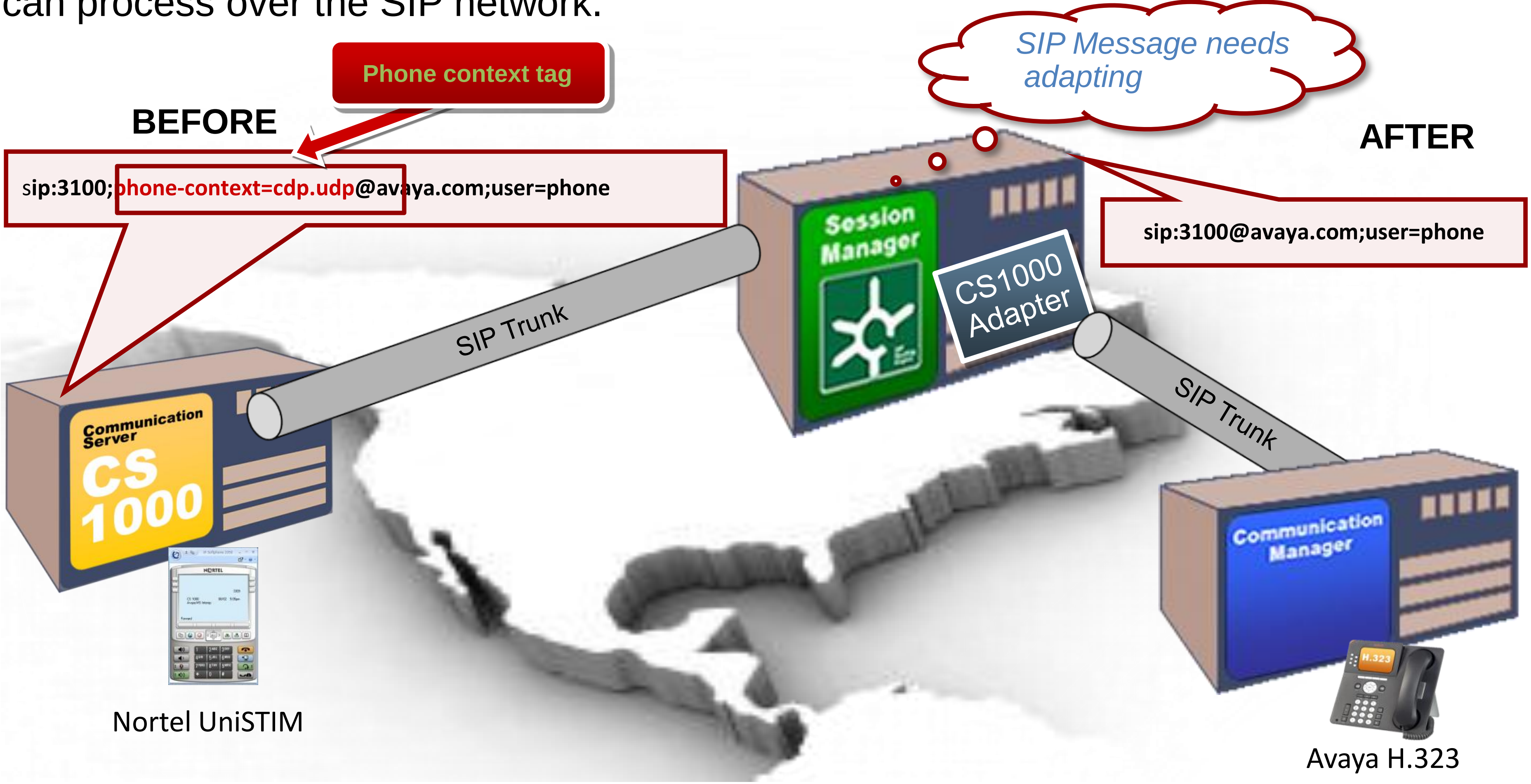
* Adaptation name:	CS1000Adapter
New module name:	CS100Adapter
Module parameter:	
Egress URI Parameters:	
Notes:	

Digit Conversion for Incoming Calls to SM

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
□	* 26	* 1	* 36	cdp.udp	* 0		destination		Removee CDPUDP Incoming

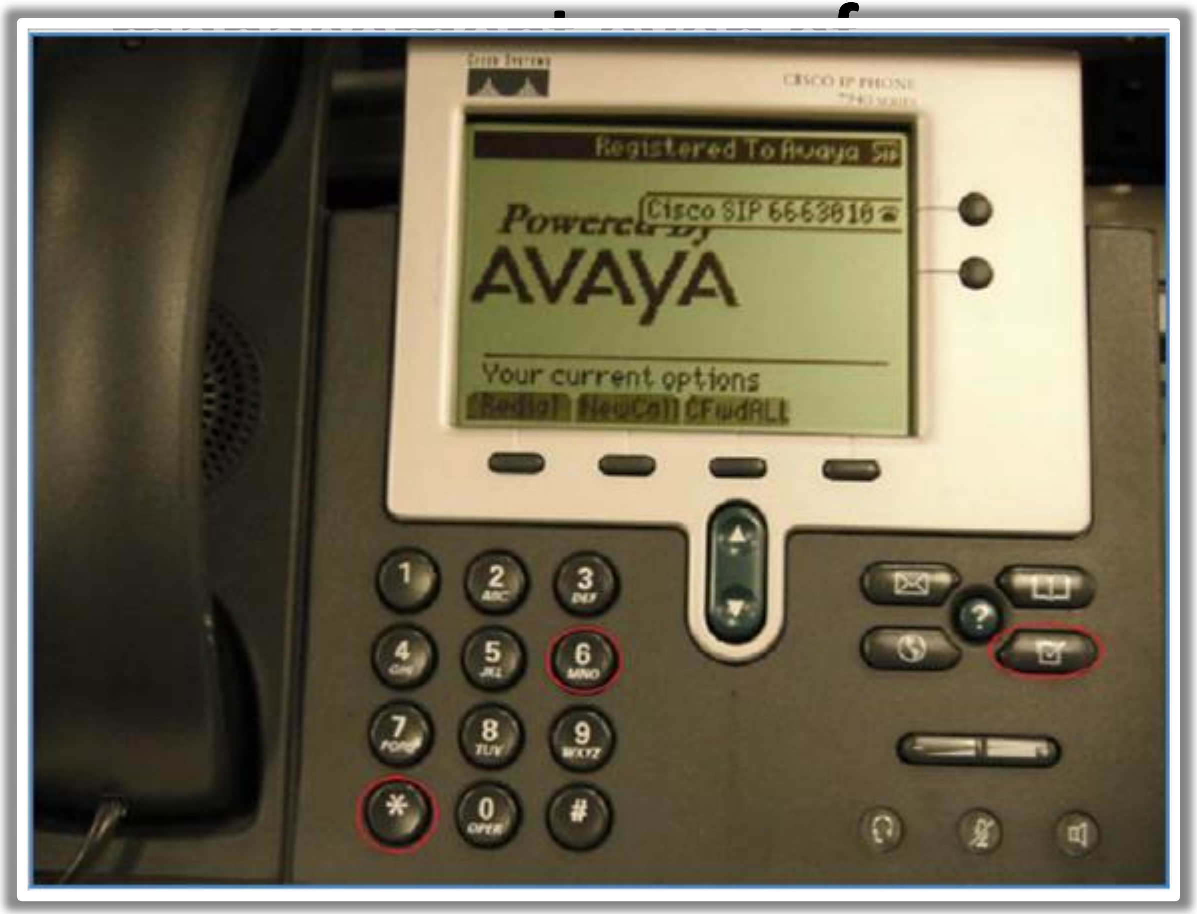
CS1000 Adapter (continued)

The CS 1000 SIP Gateway sends SIP URI messages with a “phone-context” tag in the SIP URI request message and has to be converted into a format the Session Manager can process over the SIP network.


Phone context tag
BEFORE
sip:3100;phone-context=cdp.udp@avaya.com;user=phone
SIP Message needs adapting
AFTER
sip:3100@avaya.com;user=phone
Session Manager
CS1000 Adapter
SIP Trunk
SIP Trunk
Communication Server CS 1000
Communication Manager
H.323
Nortel UniSTIM
Avaya H.323

CM-Managed Cisco Endpoint

- **Session Manager 6.2 Adaptability enables**



How is this possible?
Session Manager integrates Cisco endpoints through the use of the Cisco adaptation which now includes endpoint support!

Cisco Adaptation with Endpoint Support

Cisco SIP Messages require adaptation for the following reasons:

- Some Cisco phones require an Accept header in an inbound INVITE
- Cisco phones do not typically accept SIP messages beyond 2400 to 2800 bytes.
- Cisco firmware versions (particularly newer ones) prevents them from supporting 3rd-party proxy servers therefore Cisco phones can’t subscribe to any event packages, but they still expect OutOf Dialog-NOTIFY's to update things like message waiting lamp status.

I expect:

- Accepts header
- Small message size

Cisco Endpoint Adaptation

- ASM Adds Accept header
- Makes message smaller by stripping some headers
- ASM strips Via and Record Route headers in requests to Cisco endpoint
- ASM Sends a SUBSCRIBE on behalf of the Cisco endpoint

Cisco Endpoint Adaptation

Before

```
INVITE sip:jim@avaya.com SIP/2.0
Call-ID: -1304559591551089382##192.168.2.3
Content-Length: 118
Content-Type: application/sdp
To: sip:jim@avaya.com
From: sip:bob@avaya.com;tag=-520641854
Contact: sip:192.168.2.3:5060
RecordRoute: <sip:192.168.4.230;lr>
RecordRoute: <sip:192.168.2.210;lr>
CSeq: 1 INVITE
Max-Forwards: 70
Via: SIP/2.0/UDP 192.168.2.3:5060;branch=z9hG4bKC0
Via: SIP/2.0/UDP 192.168.2.4:5060;branch=zajifk44rrC0
Via: SIP/2.0/UDP 192.168.2.5:5060;branch=9ajdfjK9KC0

v=0
o=- 1227008289328 1227008289328 IN IP4 192.168.2.3
s=-
c=IN IP4 192.168.2.3
t=0 0
m=audio 48441 RTP/AVP 8 0
```

After w/Accept Header

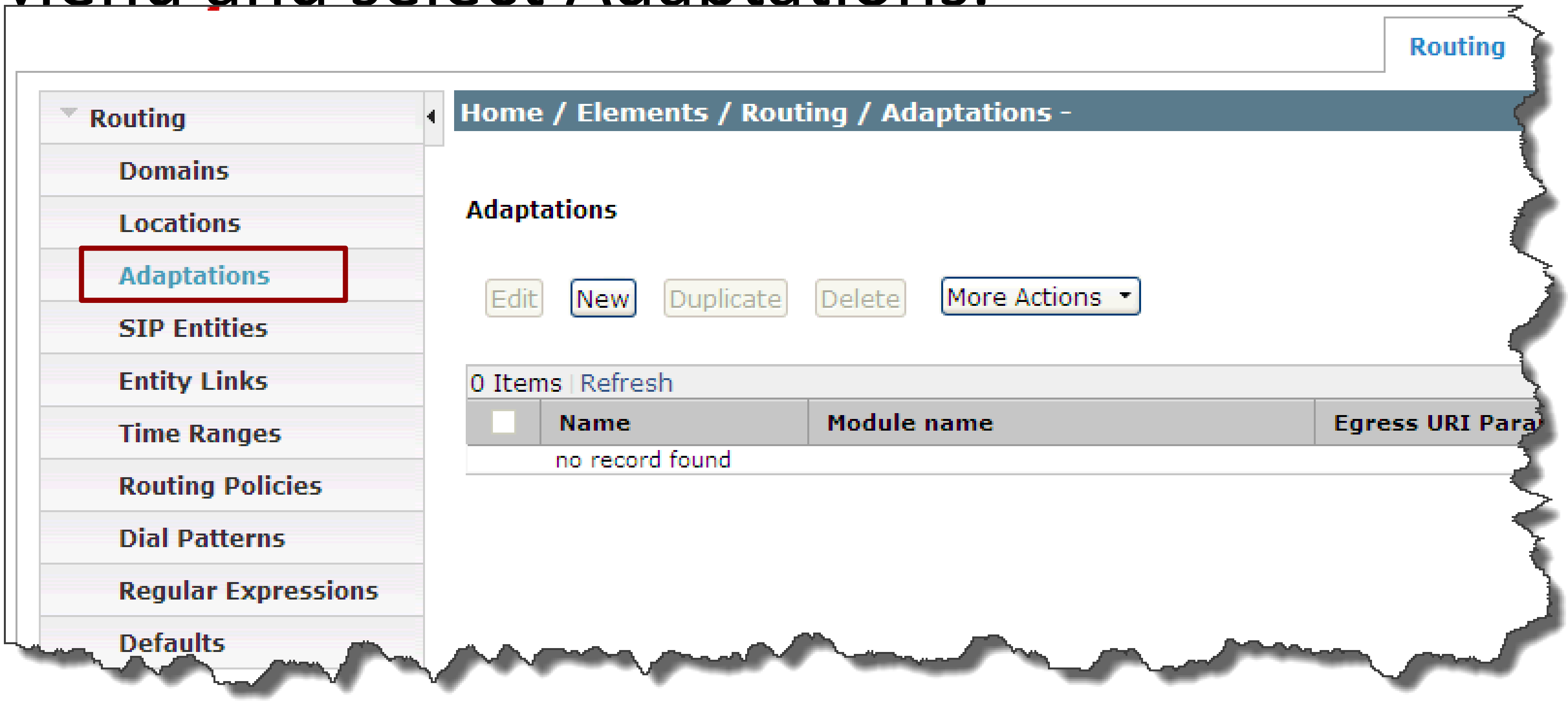
```
INVITE sip:jim@avaya.com SIP/2.0
Call-ID: -1304559591551089382##192.168.2.3
Content-Length: 118
Content-Type: application/sdp
To: sip:jim@avaya.com
From: sip:bob@avaya.com;tag=-520641854
Contact: sip:192.168.2.3:5060
RecordRoute: sip:192.168.4.230;lr
CSeq: 1 INVITE
Accept: application/sdp
Max-Forwards: 70
Via: SIP/2.0/UDP 192.168.2.3:5060;branch=z9hG4bKC0

v=0
o=- 1227008289328 1227008289328 IN IP4 192.168.2.3
s=-
c=IN IP4 192.168.2.3
t=0 0
m=audio 48441 RTP/AVP 8 0
```

AVAYA | LEARNING

Create an Adaptation

Creating Adaptations

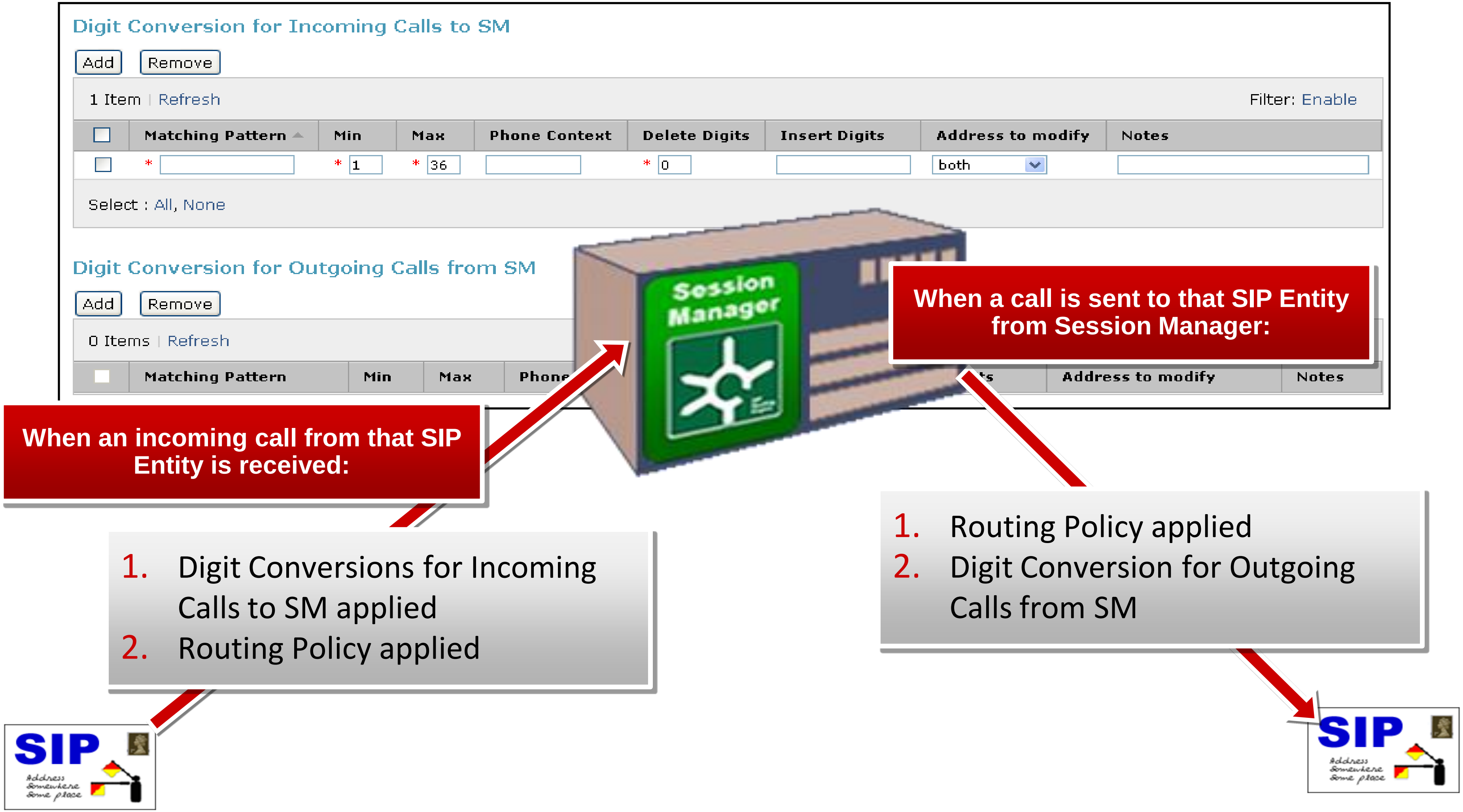
- To create an adaptation, navigate to the Routing Menu and select Adaptations.



□	Name	Module name	Egress URI Para
	no record found		

Application of Adaptations

Adaptation is created and applied to a SIP Entity.



Digit Conversion for Incoming Calls to SM

Add | Remove

1 Item | Refresh — Filter: Enable

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
□	*	* 1	* 36		* 0		both	

Select : All, None

Digit Conversion for Outgoing Calls from SM

Add | Remove

0 Items | Refresh

□	Matching Pattern	Min	Max	Phone	ts	Address to modify	Notes

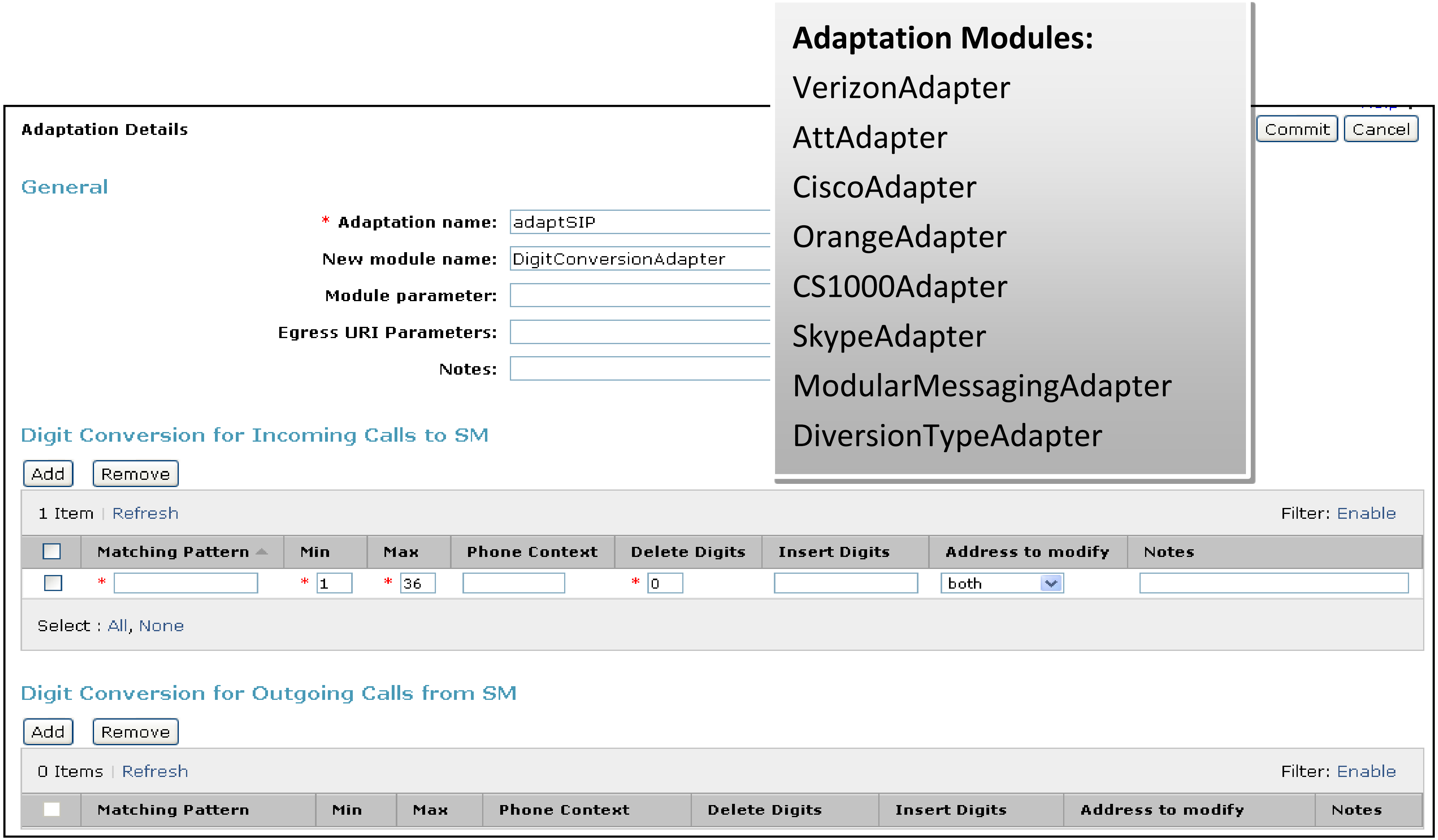
When an incoming call from that SIP Entity is received:

1. Digit Conversions for Incoming Calls to SM applied
2. Routing Policy applied

When a call is sent to that SIP Entity from Session Manager:

1. Routing Policy applied
2. Digit Conversion for Outgoing Calls from SM

Adaptations



Adaptation Modules:

VerizonAdapter

AttAdapter

CiscoAdapter

OrangeAdapter

CS1000Adapter

SkypeAdapter

ModularMessagingAdapter

DiversionTypeAdapter

Adaptation Details

General

* Adaptation name:	adaptSIP
New module name:	DigitConversionAdapter
Module parameter:	
Egress URI Parameters:	
Notes:	

Digit Conversion for Incoming Calls to SM

1 Item | Refresh Filter: Enable

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
□	*	* 1	* 36		* 0		both	

Select : All, None

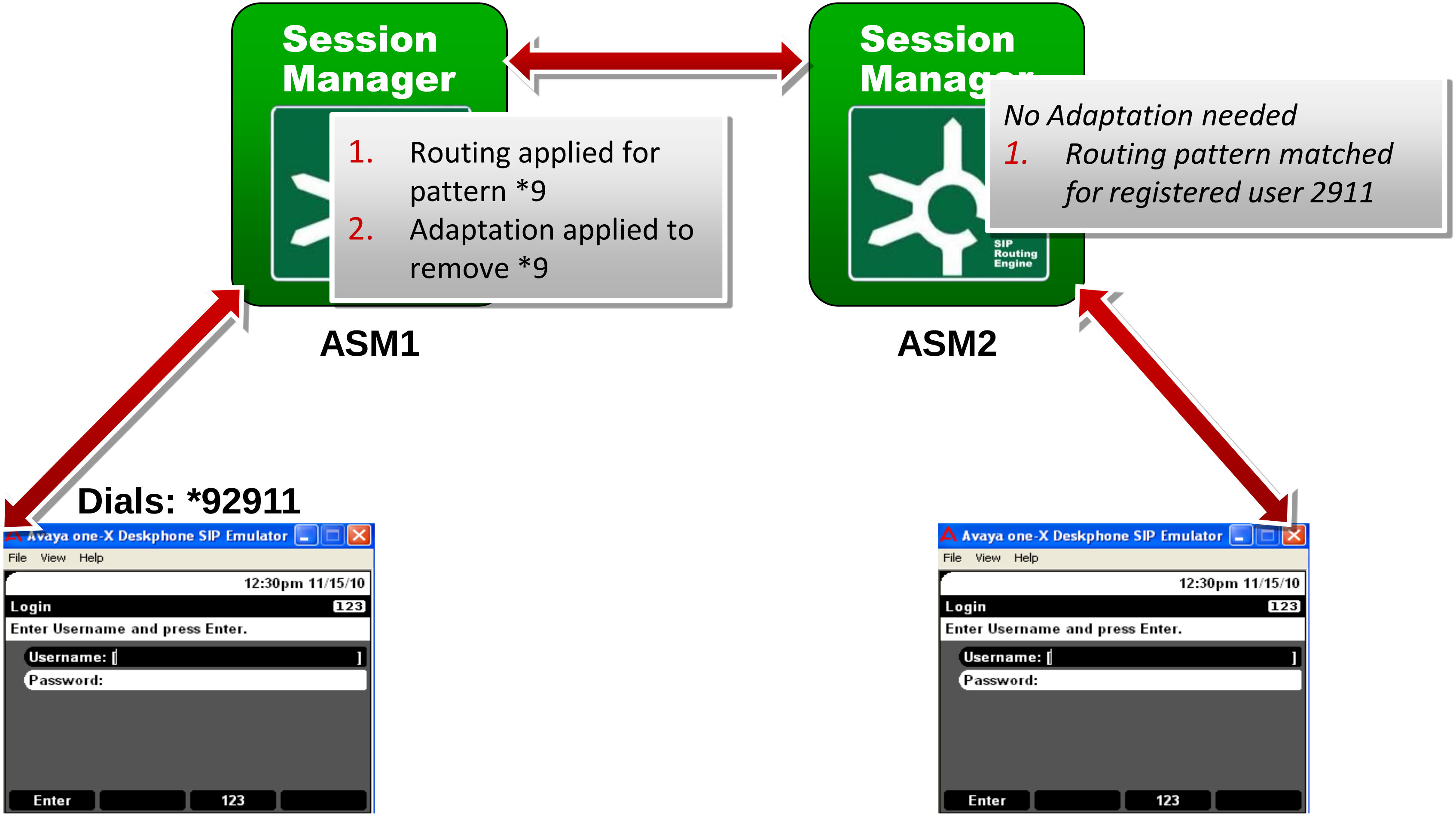
Digit Conversion for Outgoing Calls from SM

0 Items | Refresh Filter: Enable

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes

SIP to SIP Calls with Adaptations

SIP-to-SIP Routing w/Adaptation



1. Routing applied for pattern *9
2. Adaptation applied to remove *9

No Adaptation needed

1. *Routing pattern matched for registered user 2911*

Registered SIP User 1911

Registered SIP User 2911

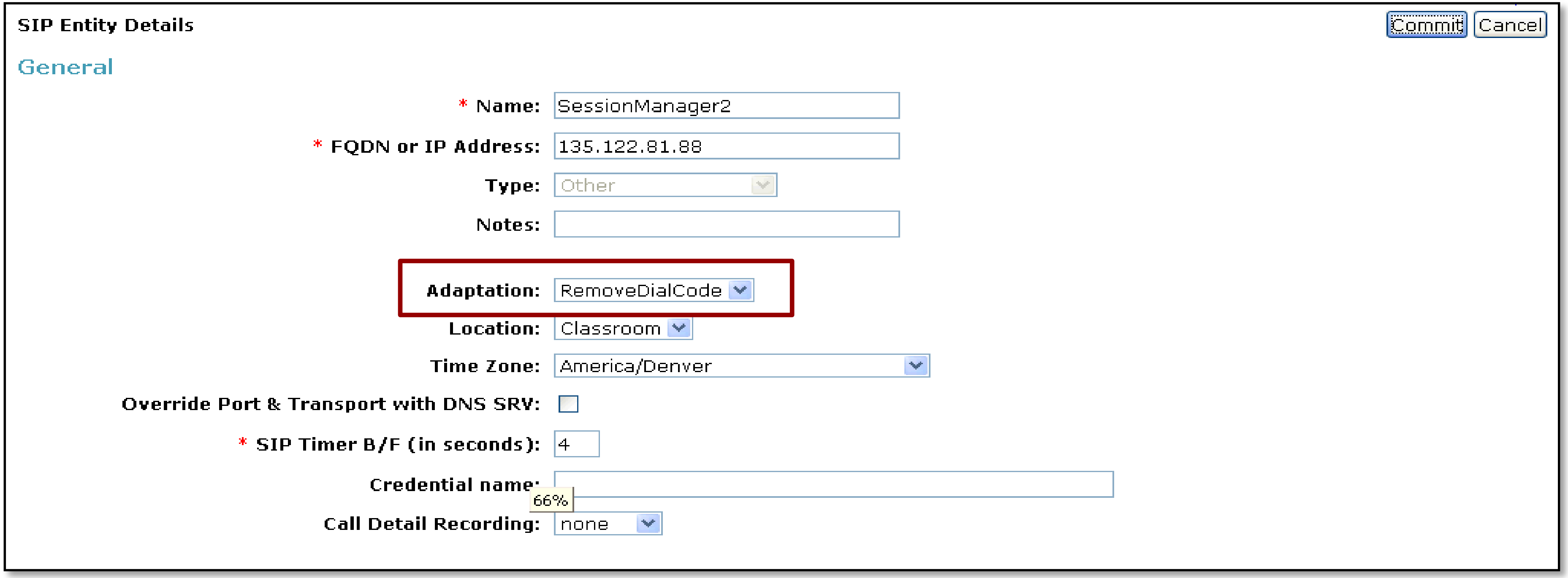
Exercise: Create Adaptation

This is a shared exercise and will require students to shadow and view each other's changes.

Step	Action
1	Create a new Adaptation called: **Remove Dial Code**
2	Module Name: ***DigitConversionAdapter***
3	Click Add below Digit Conversion for Outgoing Calls from SM to remove a ' ***9** ' from a 6 digit destination address.
4	Matching Pattern: ***9**
5	Min/Max: **6**
6	Delete Digits: **2**
7	Address to Modify: **Destination**
8	***Commit***

Applying Adaptations

Once the Adaptation is created, it can be applied to ‘far end’ SIP Entities. Adaptations CANNOT be applied to SIP Entities defined as type ‘Session Manager’.



SIP Entity Details

General

* Name:	SessionManager2
* FQDN or IP Address:	135.122.81.88
Type:	Other
Notes:	
Adaptation:	RemoveDialCode
Location:	Classroom
Time Zone:	America/Denver
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

Exercise: Place a SIP to SIP call using the Adaptation

Discuss what is required to complete this routing:

- Students will dial *9x911 or *9x921)

The *9 will be used to determine the routing but should be removed prior to the request being sent to your Neighbor’s Session Manager.

What configuration still needs to be done??

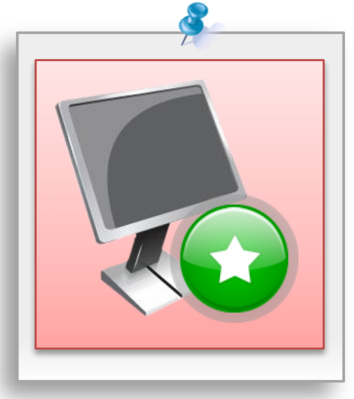
- Assume the same SIP Domain and Location are used.

Consider the following:

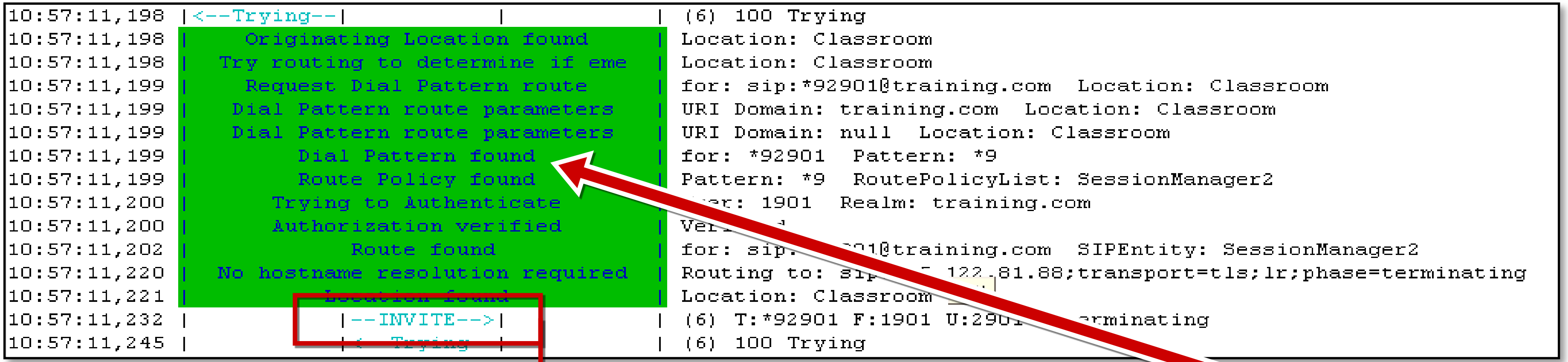
- Does your Session Manager:
  - ~~Have a trusted SIP Entity for your partner’s Session Manager?~~
  - ~~Know how to communicate with your partner’s Session Manager?~~
  - ~~Have a way to route the request to your partner’s Session Manager?~~
  - Know what dial plan to match to route to your partner’s Session Manager?
- Test using the SIP Phone Emulator to configure and log in if you haven’t done so already)
- Register as your x911 User
- Use traceSM to trace the call.

Exercise cont: Summary of Configuration Required

Step	Action
1	~~Create a SIP Entity for Partner's Session Manager (type- Other)~~ **Done**
2	~~SIP Entity Link for Partner's Session Manager~~ **Done**
3	Apply adaptation to Session Manager SIP Entity
4	~~Create Routing Policy to Partner's Session Manager~~ **Done**
5	Create Dial Pattern for your partner *9x91 Students in Pods 1 and 2 will create dial patterns for each other Students in Pods 3 and 4 will create dial patterns for each other Students in Pods 5 and 6 will create dial patterns for each other
6	Assign Routing Policy to Dial Patterns
7	Commit



traceSM – What to Look for?

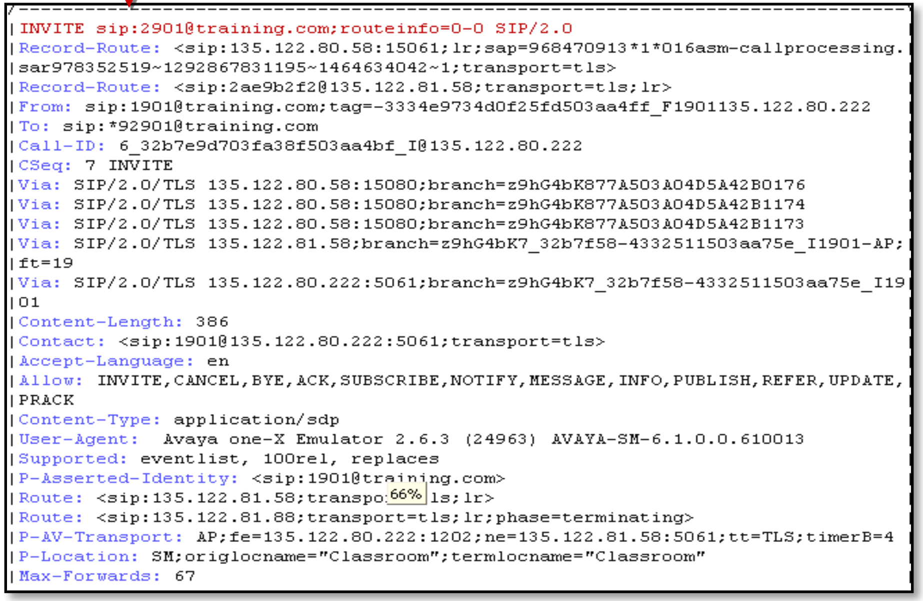


```
10:57:11,198 |<--Trying--|            |          | (6) 100 Trying
10:57:11,198 |   Originating Location found        | Location: Classroom
10:57:11,198 | Try routing to determine if eme     | Location: Classroom
10:57:11,199 |   Request Dial Pattern route        | for: sip:*92901@training.com  Location: Classroom
10:57:11,199 |  Dial Pattern route parameters      | URI Domain: training.com  Location: Classroom
10:57:11,199 |  Dial Pattern route parameters      | URI Domain: null  Location: Classroom
10:57:11,199 |       Dial Pattern found            | for: *92901  Pattern: *9
10:57:11,199 |       Route Policy found            | Pattern: *9  RoutePolicyList: SessionManager2
10:57:11,200 |     Trying to Authenticate          | User: 1901  Realm: training.com
10:57:11,200 |     Authorization verified          | Verified
10:57:11,202 |           Route found               | for: sip:*92901@training.com  SIPEntity: SessionManager2
10:57:11,220 | No hostname resolution required     | Routing to: sip:135.122.81.88;transport=tls;lr;phase=terminating
10:57:11,221 |         Location found              | Location: Classroom
10:57:11,232 |            |--INVITE-->|            | (6) T:*92901 F:1901 U:2901 [illegible]terminating
10:57:11,245 |            |<--Trying--|            | (6) 100 Trying
```

Request URI is changed, no *9.

To: remains unchanged.

Matches Dial Pattern *9 and finds Routing Policy.

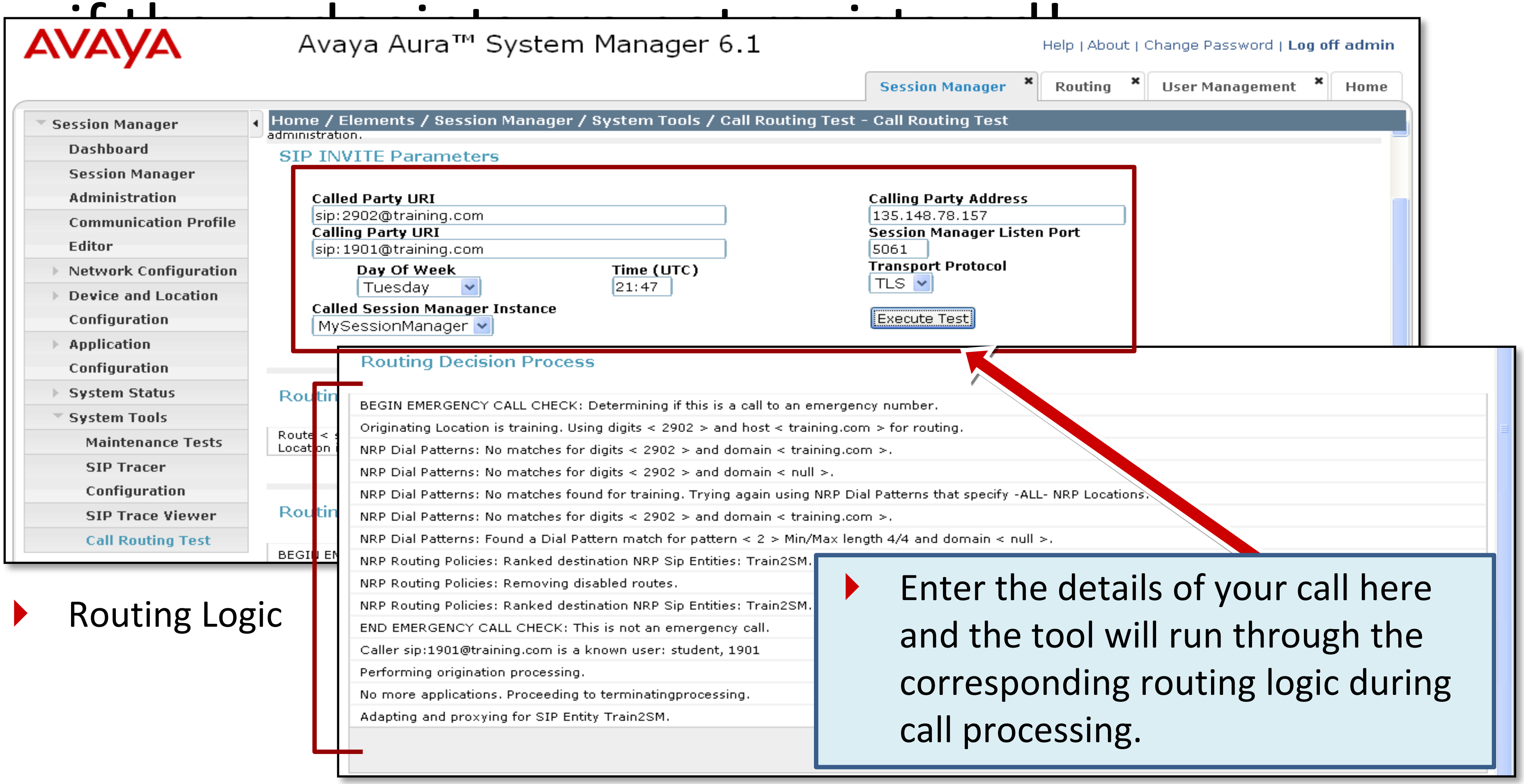


```
|INVITE sip:2901@training.com;routeinfo=0-0 SIP/2.0
|Record-Route: <sip:135.122.80.58:15061;lr;sap=968470913*1*016asm-callprocessing.
|sar978352519~1292867831195~1464634042~1;transport=tls>
|Record-Route: <sip:2ae9b2f2@135.122.81.58;transport=tls;lr>
|From: sip:1901@training.com;tag=-3334e9734d0f25fd503aa4ff_F1901135.122.80.222
|To: sip:*92901@training.com
|Call-ID: 6_32b7e9d703fa38f503aa4bf_I@135.122.80.222
|CSeq: 7 INVITE
|Via: SIP/2.0/TLS 135.122.80.58:15080;branch=z9hG4bK877A503A04D5A42B0176
|Via: SIP/2.0/TLS 135.122.80.58:15080;branch=z9hG4bK877A503A04D5A42B1174
|Via: SIP/2.0/TLS 135.122.80.58:15080;branch=z9hG4bK877A503A04D5A42B1173
|Via: SIP/2.0/TLS 135.122.81.58;branch=z9hG4bK7_32b7f58-4332511503aa75e_I1901-AP;
|ft=19
|Via: SIP/2.0/TLS 135.122.80.222:5061;branch=z9hG4bK7_32b7f58-4332511503aa75e_I19
|01
|Content-Length: 386
|Contact: <sip:1901@135.122.80.222:5061;transport=tls>
|Accept-Language: en
|Allow: INVITE,CANCEL,BYE,ACK,SUBSCRIBE,NOTIFY,MESSAGE,INFO,PUBLISH,REFER,UPDATE,
|PRACK
|Content-Type: application/sdp
|User-Agent:  Avaya one-X Emulator 2.6.3 (24963) AVAYA-SM-6.1.0.0.610013
|Supported: eventlist, 100rel, replaces
|P-Asserted-Identity: <sip:1901@training.com>
|Route: <sip:135.122.81.58;transpo 66% ls;lr>
|Route: <sip:135.122.81.88;transport=tls;lr;phase=terminating>
|P-AV-Transport: AP;fe=135.122.80.222:1202;ne=135.122.81.58:5061;tt=TLS;timerB=4
|P-Location: SM;origlocname="Classroom";termlocname="Classroom"
|Max-Forwards: 67
```

Call Routing Test

Call Routing Test

- Tool can be used for pre-deployment testing even



AVAYA Avaya Aura™ System Manager 6.1

Home / Elements / Session Manager / System Tools / Call Routing Test - Call Routing Test

administration.

SIP INVITE Parameters

Called Party URI: sip:2902@training.com

Calling Party URI: sip:1901@training.com

Day Of Week: Tuesday

Time (UTC): 21:47

Called Session Manager Instance: MySessionManager

Calling Party Address: 135.148.78.157

Session Manager Listen Port: 5061

Transport Protocol: TLS

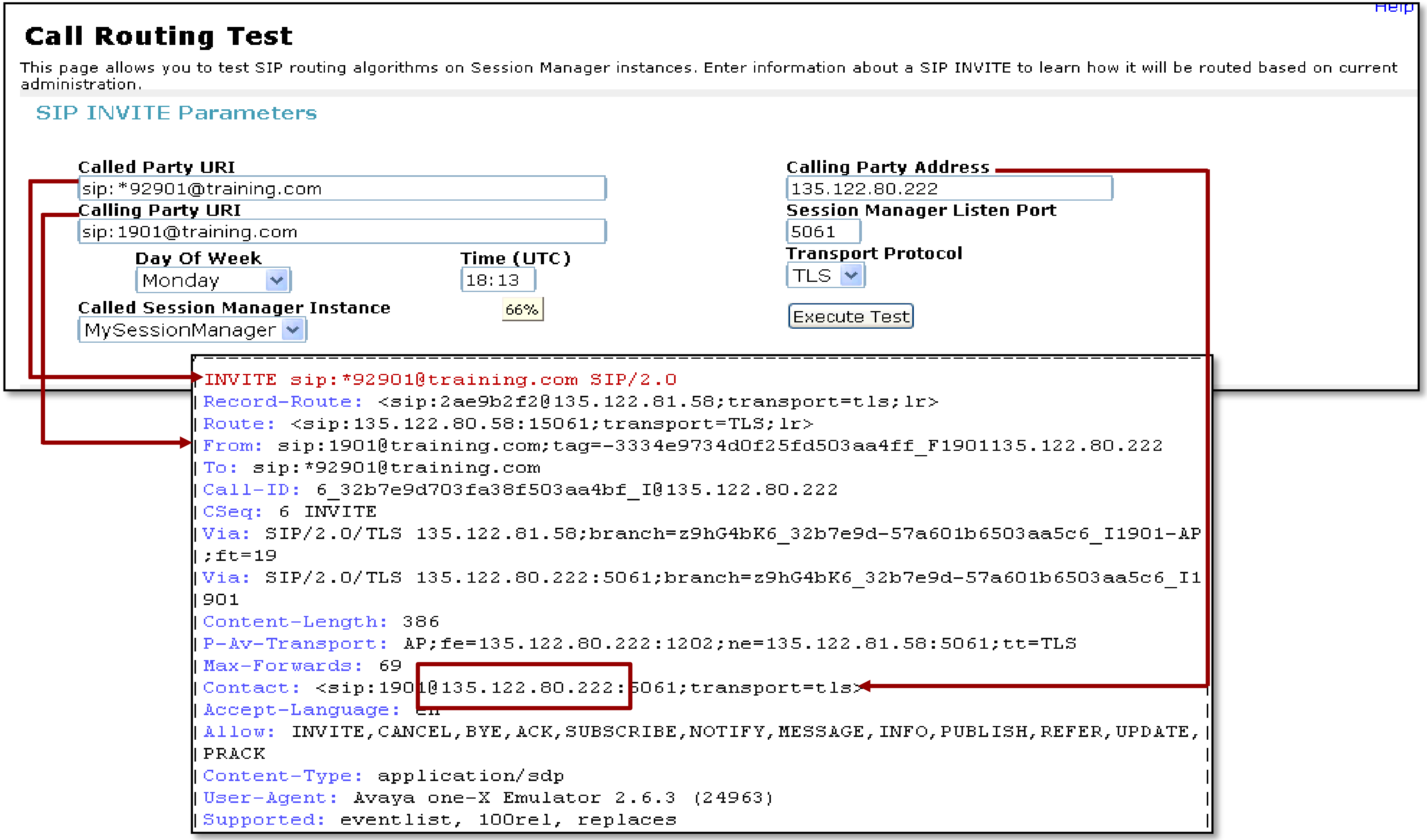
Routing Decision Process

```
BEGIN EMERGENCY CALL CHECK: Determining if this is a call to an emergency number.
Originating Location is training. Using digits < 2902 > and host < training.com > for routing.
NRP Dial Patterns: No matches for digits < 2902 > and domain < training.com >.
NRP Dial Patterns: No matches for digits < 2902 > and domain < null >.
NRP Dial Patterns: No matches found for training. Trying again using NRP Dial Patterns that specify -ALL- NRP Locations.
NRP Dial Patterns: No matches for digits < 2902 > and domain < training.com >.
NRP Dial Patterns: Found a Dial Pattern match for pattern < 2 > Min/Max length 4/4 and domain < null >.
NRP Routing Policies: Ranked destination NRP Sip Entities: Train2SM.
NRP Routing Policies: Removing disabled routes.
NRP Routing Policies: Ranked destination NRP Sip Entities: Train2SM.
END EMERGENCY CALL CHECK: This is not an emergency call.
Caller sip:1901@training.com is a known user: student, 1901
Performing origination processing.
No more applications. Proceeding to terminatingprocessing.
Adapting and proxying for SIP Entity Train2SM.
```

- Enter the details of your call here and the tool will run through the corresponding routing logic during call processing.

- Routing Logic

Call Route Testing



Call Routing Test

This page allows you to test SIP routing algorithms on Session Manager instances. Enter information about a SIP INVITE to learn how it will be routed based on current administration.

SIP INVITE Parameters

Called Party URI: sip:*92901@training.com

Calling Party URI: sip:1901@training.com

Day Of Week: Monday

Time (UTC): 18:13

Called Session Manager Instance: MySessionManager

Calling Party Address: 135.122.80.222

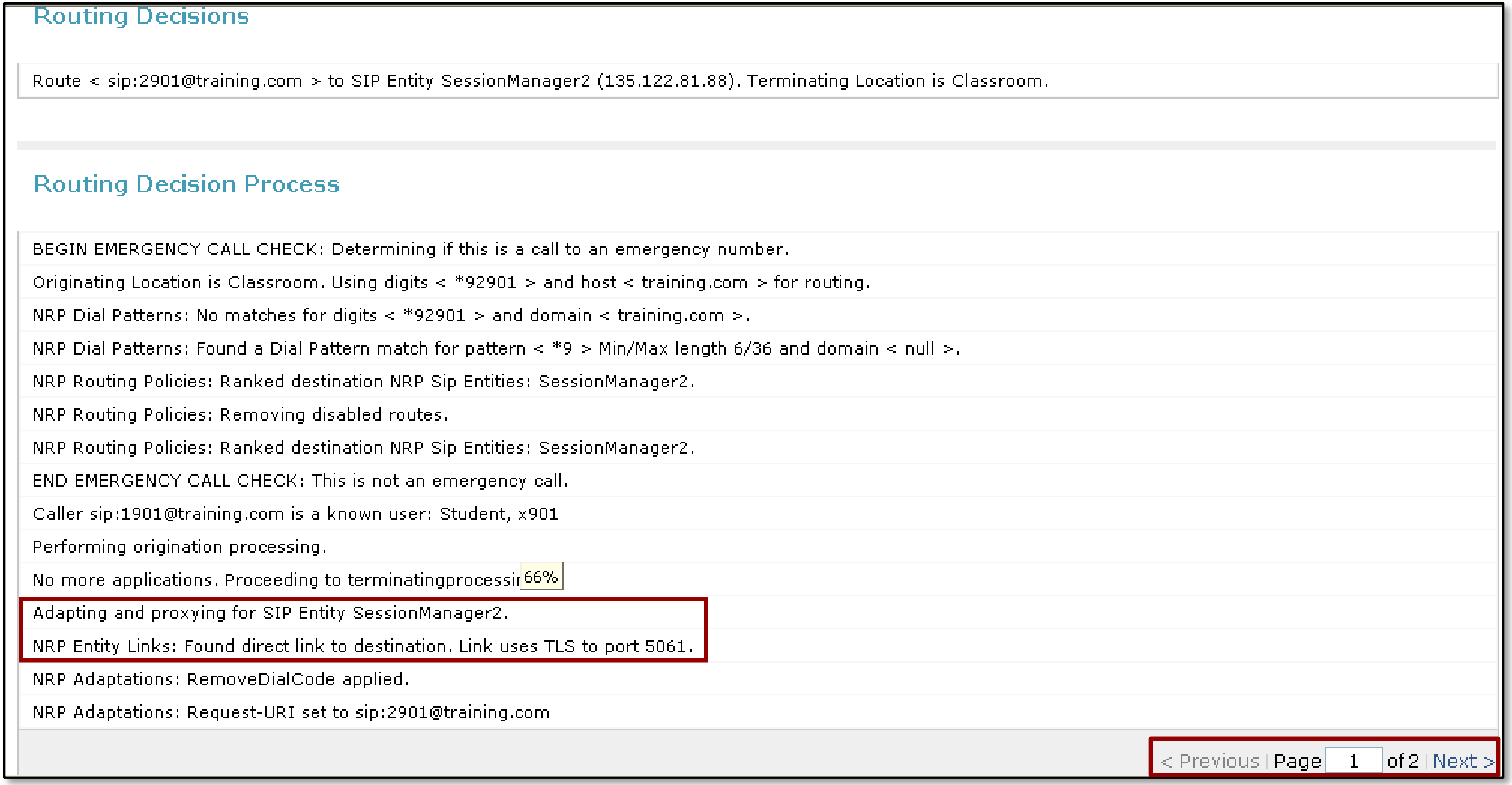
Session Manager Listen Port: 5061

Transport Protocol: TLS

```
INVITE sip:*92901@training.com SIP/2.0
Record-Route: <sip:2ae9b2f2@135.122.81.58;transport=tls;lr>
Route: <sip:135.122.80.58:15061;transport=TLS;lr>
From: sip:1901@training.com;tag=-3334e9734d0f25fd503aa4ff_F1901135.122.80.222
To: sip:*92901@training.com
Call-ID: 6_32b7e9d703fa38f503aa4bf_I@135.122.80.222
CSeq: 6 INVITE
Via: SIP/2.0/TLS 135.122.81.58;branch=z9hG4bK6_32b7e9d-57a601b6503aa5c6_I1901-AP
;ft=19
Via: SIP/2.0/TLS 135.122.80.222:5061;branch=z9hG4bK6_32b7e9d-57a601b6503aa5c6_I1
901
Content-Length: 386
P-Av-Transport: AP;fe=135.122.80.222:1202;ne=135.122.81.58:5061;tt=TLS
Max-Forwards: 69
Contact: <sip:1901@135.122.80.222:5061;transport=tls>
Accept-Language: en
Allow: INVITE,CANCEL,BYE,ACK,SUBSCRIBE,NOTIFY,MESSAGE,INFO,PUBLISH,REFER,UPDATE,
PRACK
Content-Type: application/sdp
User-Agent: Avaya one-X Emulator 2.6.3 (24963)
Supported: eventlist, 100rel, replaces
```

Call Route Testing - Results

- After **Execute Test** is clicked, the Routing Decision results are displayed.



Routing Decisions

Route < sip:2901@training.com > to SIP Entity SessionManager2 (135.122.81.88). Terminating Location is Classroom.

Routing Decision Process

BEGIN EMERGENCY CALL CHECK: Determining if this is a call to an emergency number.

Originating Location is Classroom. Using digits < *92901 > and host < training.com > for routing.

NRP Dial Patterns: No matches for digits < *92901 > and domain < training.com >.

NRP Dial Patterns: Found a Dial Pattern match for pattern < *9 > Min/Max length 6/36 and domain < null >.

NRP Routing Policies: Ranked destination NRP Sip Entities: SessionManager2.

NRP Routing Policies: Removing disabled routes.

NRP Routing Policies: Ranked destination NRP Sip Entities: SessionManager2.

END EMERGENCY CALL CHECK: This is not an emergency call.

Caller sip:1901@training.com is a known user: Student, x901

Performing origination processing.

No more applications. Proceeding to terminatingprocessir 66%

Adapting and proxying for SIP Entity SessionManager2.

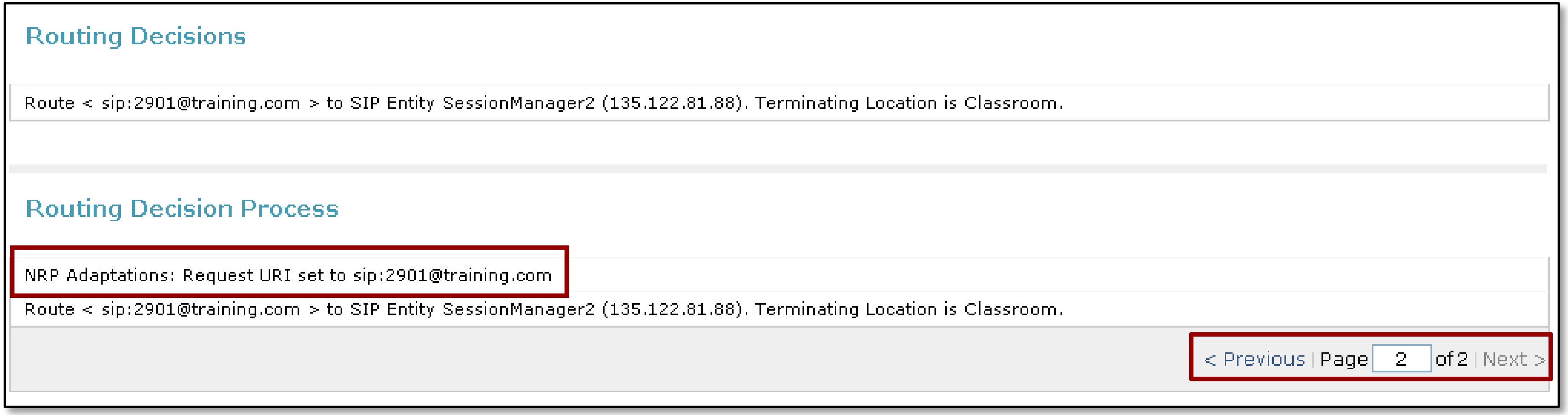
NRP Entity Links: Found direct link to destination. Link uses TLS to port 5061.

NRP Adaptations: RemoveDialCode applied.

NRP Adaptations: Request-URI set to sip:2901@training.com

Call Route Testing – Results (continued)

Page 2 of the Routing Decision Results



Routing Decisions

Route < sip:2901@training.com > to SIP Entity SessionManager2 (135.122.81.88). Terminating Location is Classroom.

Routing Decision Process

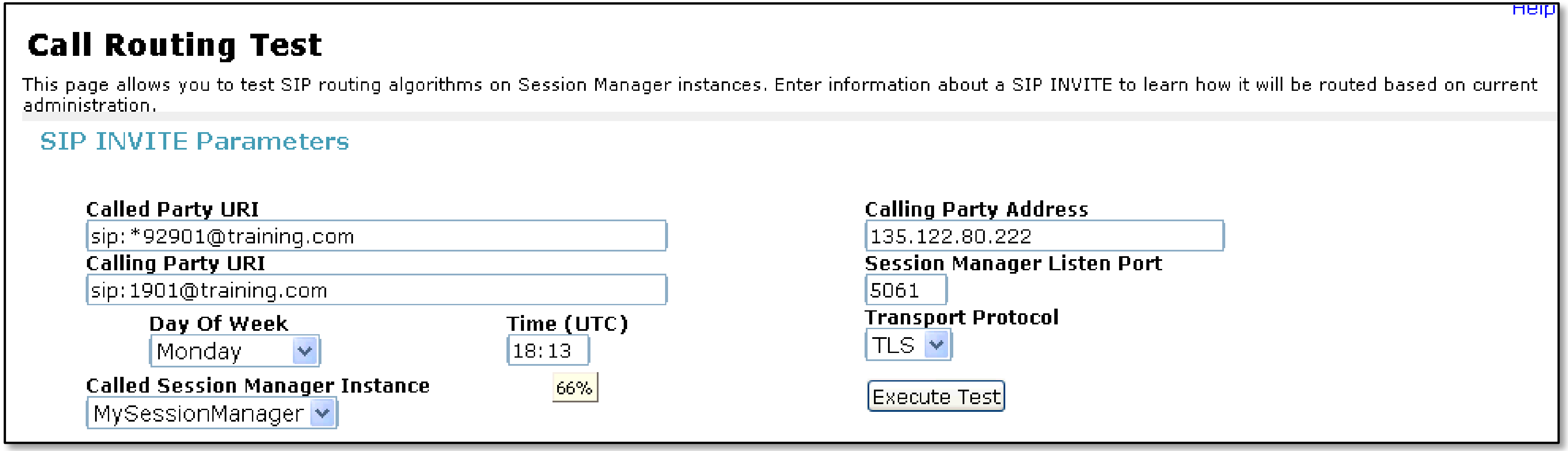
NRP Adaptations: Request URI set to sip:2901@training.com

Route < sip:2901@training.com > to SIP Entity SessionManager2 (135.122.81.88). Terminating Location is Classroom.

Exercise: Call Routing Test

Use the Call Routing Test Tool to simulate th

Step	Action
1	Navigate to Elements Column >> Session Manager >> System Tools>> Call Routing Test
2	Enter the call details: called party URI, calling party URI (you), calling party Address (your desktop IP: 172.16.1.11/12, Called Session Manager Instance
3	Execute Test



Call Routing Test

This page allows you to test SIP routing algorithms on Session Manager instances. Enter information about a SIP INVITE to learn how it will be routed based on current administration.

SIP INVITE Parameters

Called Party URI: sip:*92901@training.com

Calling Party URI: sip:1901@training.com

Day Of Week: Monday

Time (UTC): 18:13

Called Session Manager Instance: MySessionManager

Calling Party Address: 135.122.80.222

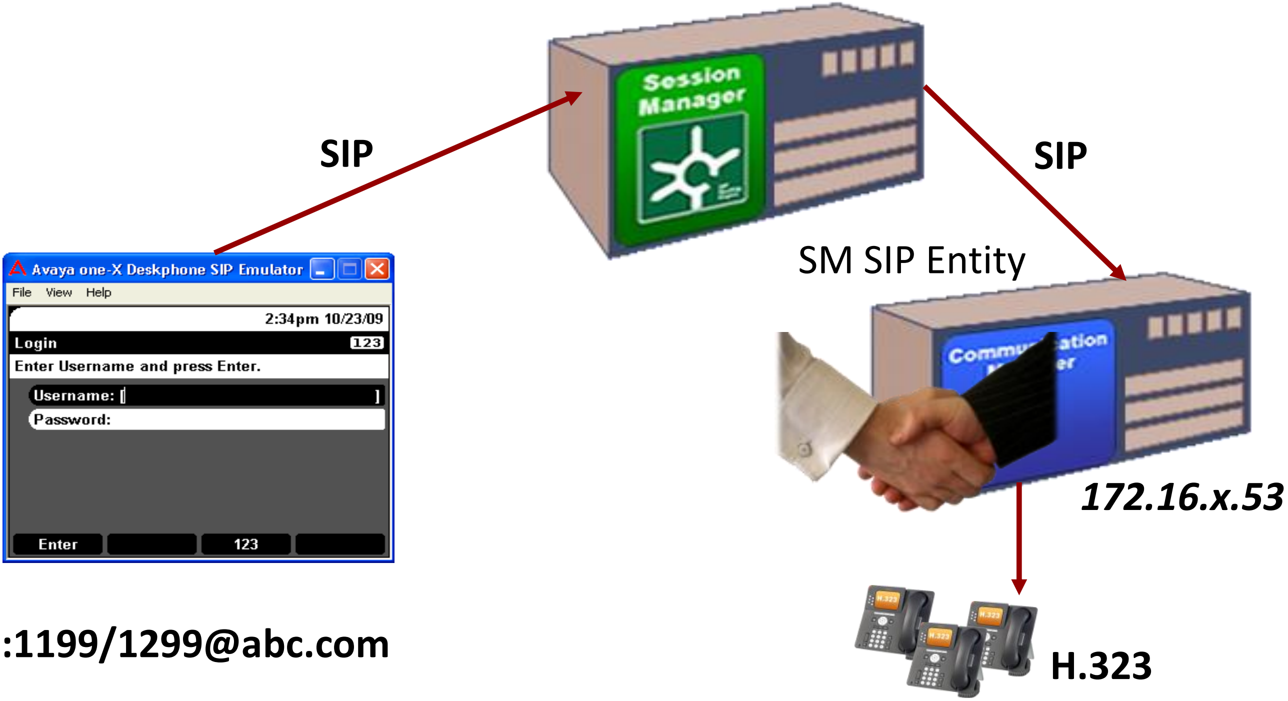
Session Manager Listen Port: 5061

Transport Protocol: TLS

AVAYA | LEARNING

SIP to H.323 Calling within Different Domains

SIP Phone to H.323 Phone within Different Domains



Avaya one-X Deskphone SIP Emulator

File View Help

2:34pm 10/23/09

Login 123

Enter Username and press Enter.

Username: [ ]

Password:

Enter 123

What additional configuration do we need to make to place this call?

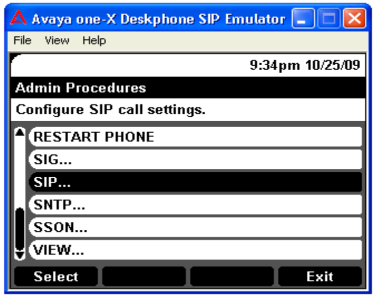
- Assume the SIP Domain (abc.com) and Location are configured.
- Does your Session Manager:
  - Recognize the CM as a SIP Entity?
  - Know how to communicate with CM?
  - Recognize the registered SIP User? – Yes, it has been created for you.

Exercise: Create User Communication Profile x199/x299 in abc.com domain

Step	Action
1	At System Manager console select User Management Menu
2	Select ***New***
3	**On the Identity Tab:** ● Add First/Last Name: Your name ● Login Name: email address format i.e. **yourname@avaya.com** ● Password: **Passw0rd!**
4	**On the Communication Profile Tab:** Password: Enter **123456** ● Go down to Communication Address ● Select ***New*** ● Select: ***Avaya SIP*** ● Fully qualified address : Student a= **x199@abc.com** Student b = **x299@abc.com** Select ***Add***
5	**Session Manager Profile** Assign the user to your assigned Session Manager Location: **Denver**
6	***Commit*** your changes

Exercise: Prepare x199/x299 SIP Phone

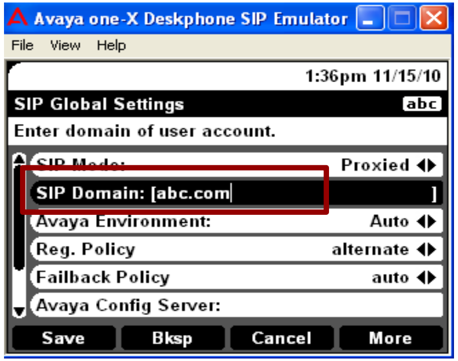
Step	Action
1	Open another instance of the **SIP Emulator #3**
2	*Navigate to View >> Admin Options*
3	*Make sure in **ADDR** menu is the **172.16.x.11** or **.12** IP address*
4	*Select **SIG** Menu and enter **SIP***
5	Use your down or up **Arrow Key** until SIP is highlighted and press **Enter**
6	SIP Global Settings is highlighted, press **Enter** ● SIP Mode = ***Proxied*** ● SIP Domain = **abc.com**
7	Click **Save**
8	● Use your down or up **Arrow Key** until SIP Proxy Settings is highlighted and press **Enter**
9	● Click existing SIP Proxy Change SIP Port = **5062**
10	Click **Save, Back, Back, Logoff**
11	Do not Select Exit!!!!
12	Log into x199/x299



9:34pm 10/25/09

Admin Procedures

Configure SIP call settings.



1:36pm 11/15/10

SIP Global Settings

Enter domain of user account.

SIP Mode: Proxied

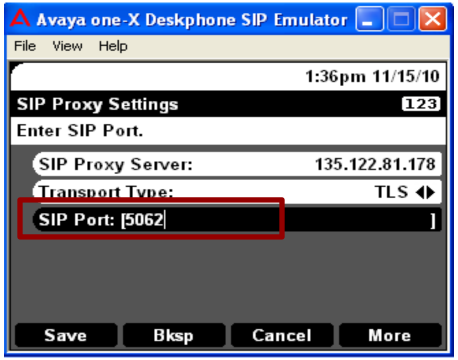
SIP Domain: [abc.com]

Avaya Environment: Auto

Reg. Policy alternate

Failback Policy auto

Avaya Config Server:



1:36pm 11/15/10

SIP Proxy Settings

Enter SIP Port.

SIP Proxy Server: 135.122.81.178

Transport Type: TLS

SIP Port: [5062]

Exercise: Place a Call via SIP User to CM IP Station

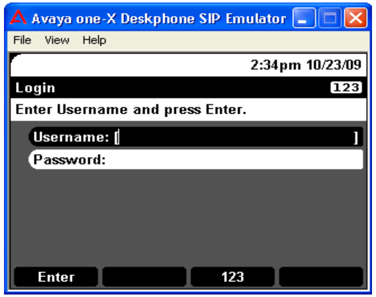
Log into your x711/x721 IP Station

Log into your x199/x299 SIP Phone

Test

Was it successful?

Student	Pod 1	Pod 2	Pod 3	Pod 4	Pod 5	Pod 6
Student a	1711	3711	1711	3701	1701	3701
Student b	2721	4721	2721	4701	2701	4701



Avaya one-X Deskphone SIP Emulator

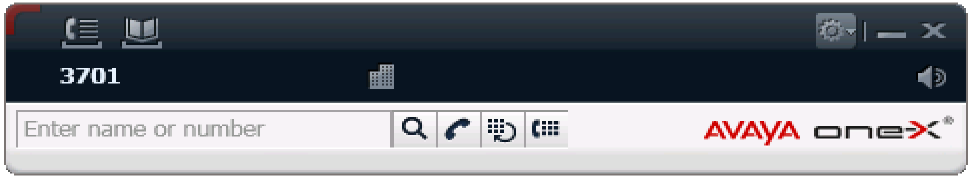
2:34pm 10/23/09

Login 123

Enter Username and press Enter.

Username: [

Password:

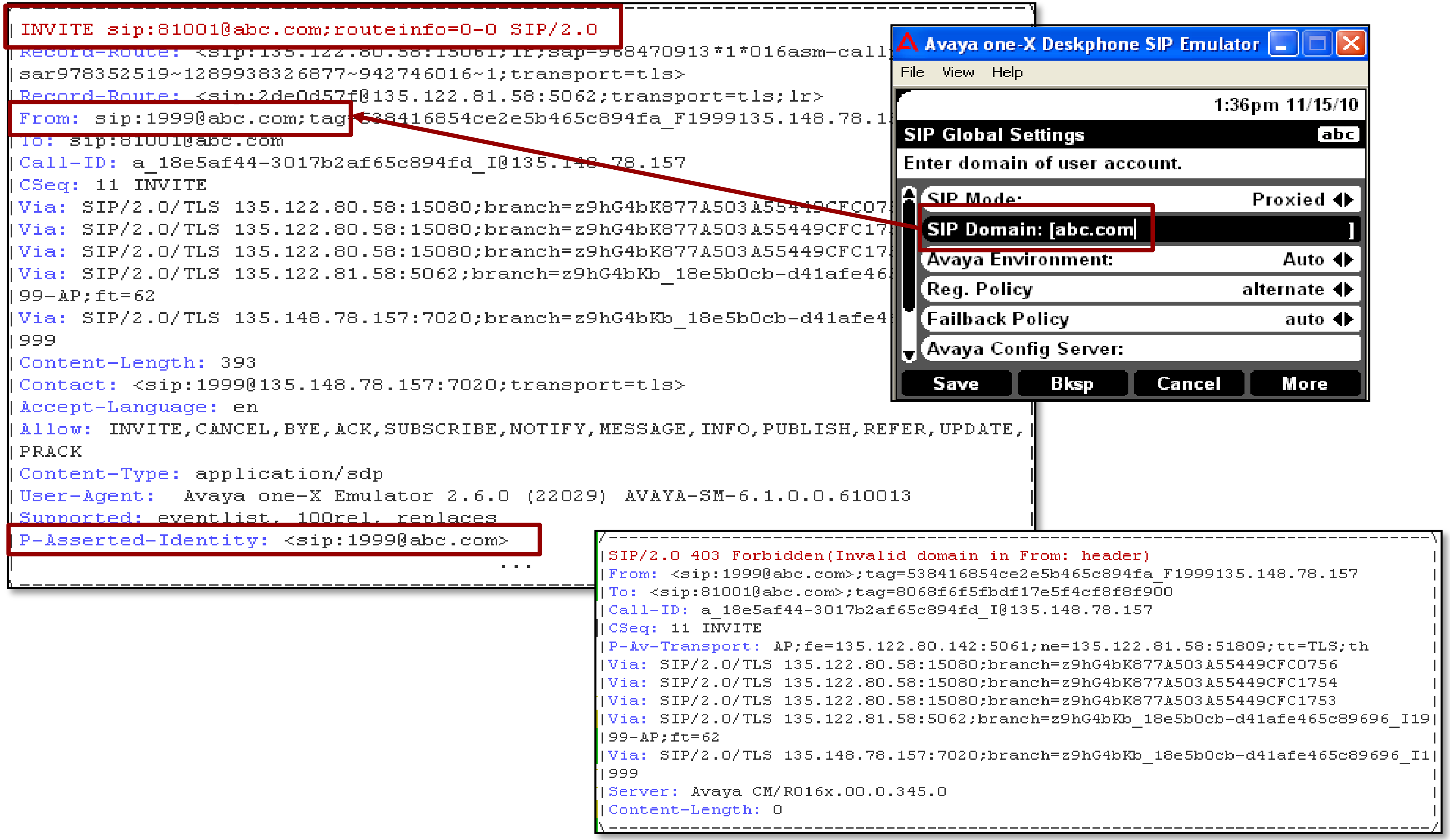


3701

Enter name or number

Student	Pod 1	Pod 2	Pod 3	Pod 4	Pod 5	Pod 6
Student a	1199	2199	3199	4199	5199	6199
Student b	1299	2299	3299	4299	5299	6299

403 Forbidden: Invalid Domain in From Header



```
| INVITE sip:81001@abc.com;routeinfo=0-0 SIP/2.0
|Record-Route: <sip:135.122.80.58:15061;lr;sap=968470913*1*016asm-call
|sar978352519~1289938326877~942746016~1;transport=tls>
|Record-Route: <sip:2de0d57f@135.122.81.58:5062;transport=tls;lr>
|From: sip:1999@abc.com;tag=538416854ce2e5b465c894fa_F1999135.148.78.1
|To: sip:81001@abc.com
|Call-ID: a_18e5af44-3017b2af65c894fd_I@135.148.78.157
|CSeq: 11 INVITE
|Via: SIP/2.0/TLS 135.122.80.58:15080;branch=z9hG4bK877A503A55449CFC07
|Via: SIP/2.0/TLS 135.122.80.58:15080;branch=z9hG4bK877A503A55449CFC17
|Via: SIP/2.0/TLS 135.122.80.58:15080;branch=z9hG4bK877A503A55449CFC17
|Via: SIP/2.0/TLS 135.122.81.58:5062;branch=z9hG4bKb_18e5b0cb-d41afe46
|99-AP;ft=62
|Via: SIP/2.0/TLS 135.148.78.157:7020;branch=z9hG4bKb_18e5b0cb-d41afe4
|999
|Content-Length: 393
|Contact: <sip:1999@135.148.78.157:7020;transport=tls>
|Accept-Language: en
|Allow: INVITE,CANCEL,BYE,ACK,SUBSCRIBE,NOTIFY,MESSAGE,INFO,PUBLISH,REFER,UPDATE,|
|PRACK                                                                           |
|Content-Type: application/sdp                                                   |
|User-Agent: Avaya one-X Emulator 2.6.0 (22029) AVAYA-SM-6.1.0.0.610013          |
|Supported: eventlist, 100rel, replaces
|P-Asserted-Identity: <sip:1999@abc.com>
|                                                       ...
```

Avaya one-X Deskphone SIP Emulator

File View Help

1:36pm 11/15/10

SIP Global Settings abc

Enter domain of user account.

SIP Mode:	Proxied ◆
SIP Domain: [abc.com	]
Avaya Environment:	Auto ◆
Reg. Policy	alternate ◆
Failback Policy	auto ◆
Avaya Config Server:	

```
|SIP/2.0 403 Forbidden(Invalid domain in From: header)                     |
|From: <sip:1999@abc.com>;tag=538416854ce2e5b465c894fa_F1999135.148.78.157 |
|To: <sip:81001@abc.com>;tag=8068f6f5fbdf17e5f4cf8f8f900                   |
|Call-ID: a_18e5af44-3017b2af65c894fd_I@135.148.78.157                     |
|CSeq: 11 INVITE                                                           |
|P-Av-Transport: AP;fe=135.122.80.142:5061;ne=135.122.81.58:51809;tt=TLS;th|
|Via: SIP/2.0/TLS 135.122.80.58:15080;branch=z9hG4bK877A503A55449CFC0756   |
|Via: SIP/2.0/TLS 135.122.80.58:15080;branch=z9hG4bK877A503A55449CFC1754   |
|Via: SIP/2.0/TLS 135.122.80.58:15080;branch=z9hG4bK877A503A55449CFC1753   |
|Via: SIP/2.0/TLS 135.122.81.58:5062;branch=z9hG4bKb_18e5b0cb-d41afe465c89696_I19|
|99-AP;ft=62                                                               |
|Via: SIP/2.0/TLS 135.148.78.157:7020;branch=z9hG4bKb_18e5b0cb-d41afe465c89696_I1|
|999                                                                       |
|Server: Avaya CM/R016x.00.0.345.0                                         |
|Content-Length: 0                                                         |
```

Adaptability

Adaptations can be used to change the SIP Domain in the RequestURI (destination) and the P-Asserted Identity (PAI) (source).

DigitConversionAdapter: Domain Name Change

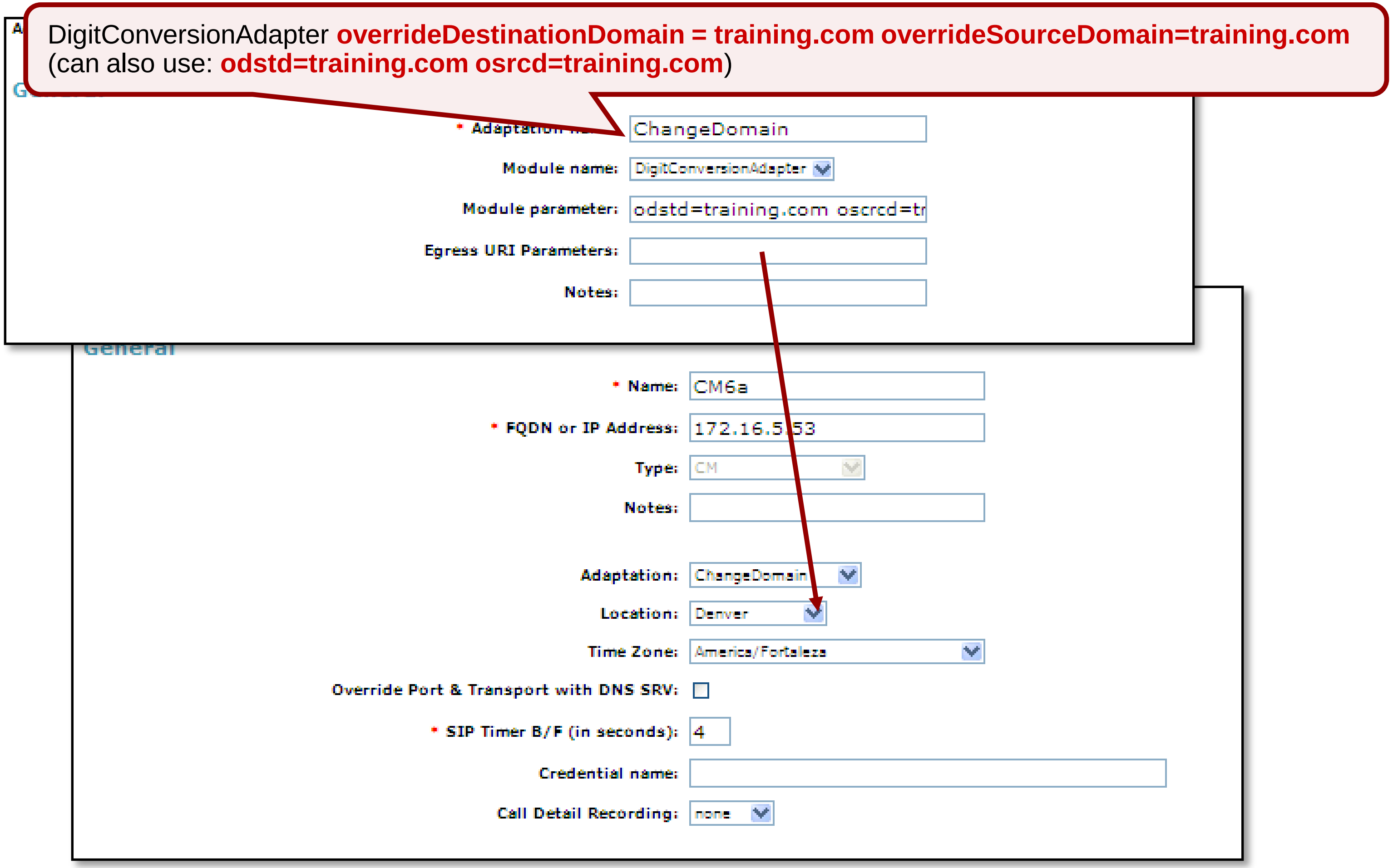
- Outbound call Domain Modification Parameter
  - overrideDestinationDomain (odstd) replaces the domain in Request-URI
  - overrideSourceDomain (osrcd): replaces the domain in the P-Asserted-Identity header
- Inbound call Domain Modification Parameters
  - ingressOverrideDestinationDomain (iodstd) replaces the domain in Request-URI
  - ingressoverrideSourceDomain (iosrcd) replaces the domain in the P-Asserted-Identity header

Example:
ModuleName:
DigitConversionAdapter

Module Parameter:
odstd=training.com
osrcd=training.com

Change Domain of Source

- The order of the module parameters in not important.
- Once the adaptation is created then it must be assigned to the SIP entity.



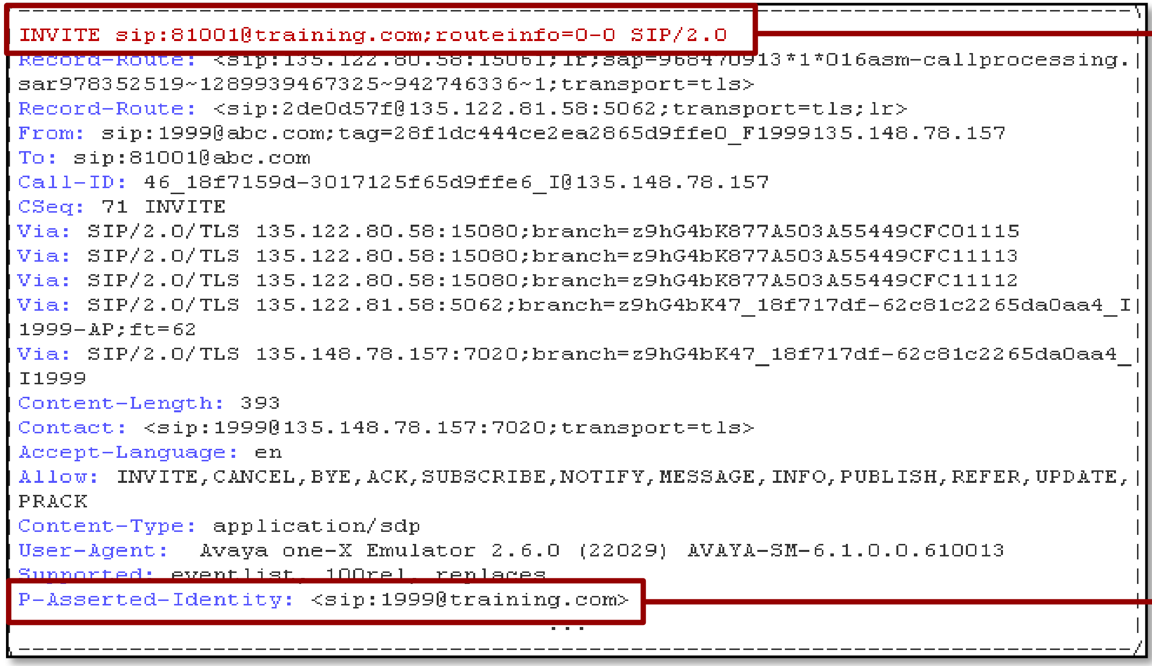
DigitConversionAdapter **overrideDestinationDomain = training.com overrideSourceDomain=training.com** (can also use: **odstd=training.com osrcd=training.com**)

* Adaptation na	ChangeDomain
Module name:	DigitConversionAdapter
Module parameter:	odstd=training.com oscrcd=tr
Egress URI Parameters:	
Notes:	

General

* Name:	CM6a
* FQDN or IP Address:	172.16.5.53
Type:	CM
Notes:	
Adaptation:	ChangeDomain
Location:	Denver
Time Zone:	America/Fortaleza
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

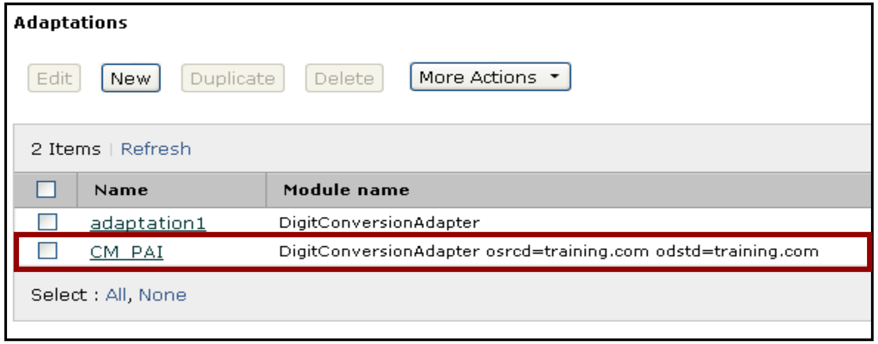
Result of Domain Change



```
INVITE sip:81001@training.com;routeinfo=0-0 SIP/2.0
Record-Route: <sip:135.122.80.58:15061;lr;sap=968470913*1*016asm-callprocessing.
sar978352519~1289939467325~942746336~1;transport=tls>
Record-Route: <sip:2de0d57f@135.122.81.58:5062;transport=tls;lr>
From: sip:1999@abc.com;tag=28f1dc444ce2ea2865d9ffe0_F1999135.148.78.157
To: sip:81001@abc.com
Call-ID: 46_18f7159d-3017125f65d9ffe6_I@135.148.78.157
CSeq: 71 INVITE
Via: SIP/2.0/TLS 135.122.80.58:15080;branch=z9hG4bK877A503A55449CFC01115
Via: SIP/2.0/TLS 135.122.80.58:15080;branch=z9hG4bK877A503A55449CFC11113
Via: SIP/2.0/TLS 135.122.80.58:15080;branch=z9hG4bK877A503A55449CFC11112
Via: SIP/2.0/TLS 135.122.81.58:5062;branch=z9hG4bK47_18f717df-62c81c2265da0aa4_I
1999-AP;ft=62
Via: SIP/2.0/TLS 135.148.78.157:7020;branch=z9hG4bK47_18f717df-62c81c2265da0aa4_
I1999
Content-Length: 393
Contact: <sip:1999@135.148.78.157:7020;transport=tls>
Accept-Language: en
Allow: INVITE,CANCEL,BYE,ACK,SUBSCRIBE,NOTIFY,MESSAGE,INFO,PUBLISH,REFER,UPDATE,
PRACK
Content-Type: application/sdp
User-Agent:  Avaya one-X Emulator 2.6.0 (22029) AVAYA-SM-6.1.0.0.610013
Supported: eventlist, 100rel, replaces
P-Asserted-Identity: <sip:1999@training.com>
                                        ...
```

odstd=training.com

osrcd=training.com

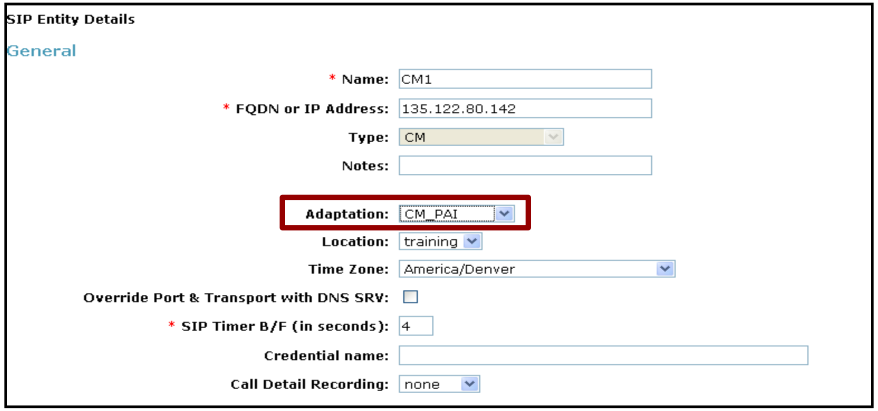


Adaptations

2 Items | Refresh

□	Name	Module name
□	adaptation1	DigitConversionAdapter
□	CM_PAI	DigitConversionAdapter osrcd=training.com odstd=training.com

Select : All, None



SIP Entity Details

General

* Name:	CM1
* FQDN or IP Address:	135.122.80.142
Type:	CM
Notes:	
Adaptation:	CM_PAI
Location:	training
Time Zone:	America/Denver
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

Exercise: Define an Adaptation to change the Source and Destination SIP Domain from abc.com to training.com

Step	Action
1	Create a new Adaptation called '***ChangeDomain***' using the DigitConversionAdapter Module and apply to the CM SIP Entity.
2	Student A: Add Outbound Module Parameters to change the: Destination SIP Domain to training.com **odstd= training.com**
3	Source SIP Domain to training.com **osrcd=training.com**
4	Student B: Apply the adaptation to your CM SIP entity
5	Test Place the actual call and view traceSM Use the Call Routing Test tool to see the Adaptation

Only one adaptation is configured per Pod.

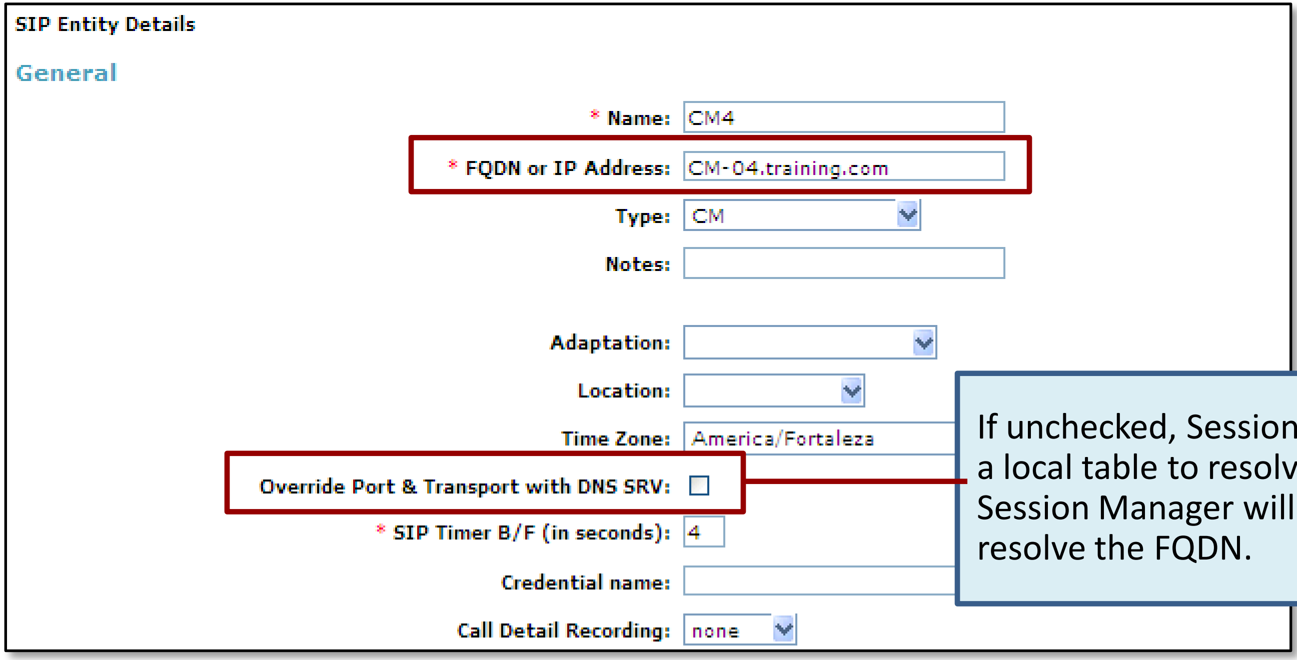
This is a shared exercise and will require students to shadow and view each other's changes.

AVAYA | LEARNING

Local Host Name Resolution

Local Host Name Resolution

- Session Manager has an internal host table for resolving a host name to a specific IP address.
- Can add one SIP Entity FQDN and IP addresses of multiple instances of that SIP Entity for load balancing



SIP Entity Details

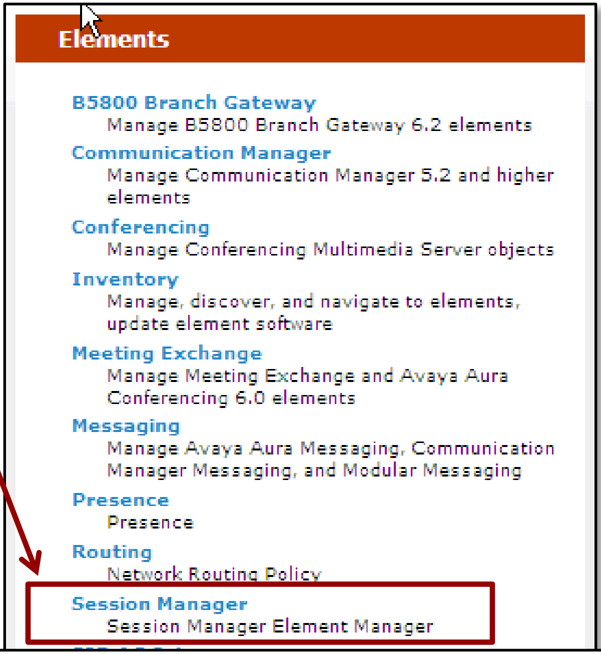
General

* Name:	CM4
* FQDN or IP Address:	CM-04.training.com
Type:	CM
Notes:	
Adaptation:	
Location:	
Time Zone:	America/Fortaleza
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

If unchecked, Session Manager uses a local table to resolve. If checked, Session Manager will use DNS to resolve the FQDN.

Local Host Name Resolution (continued)

- To modify Session Manager's Local Host Name Resolution table, access the Element Menu and select Session Manager
- Select Network Configuration>>Local Host Name Resolution
- Select New



Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway 6.2 elements

Communication Manager
Manage Communication Manager 5.2 and higher elements

Conferencing
Manage Conferencing Multimedia Server objects

Inventory
Manage, discover, and navigate to elements, update element software

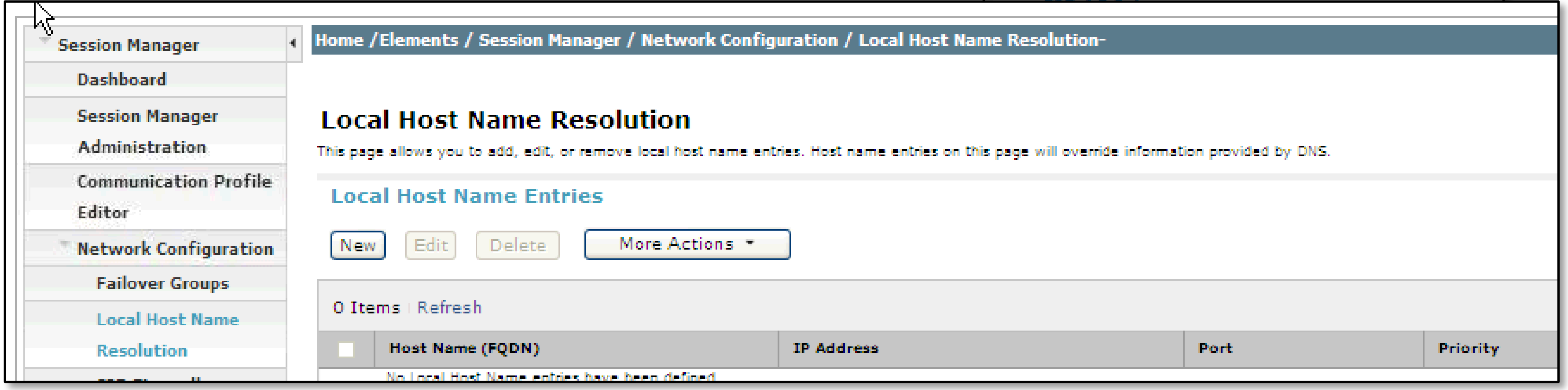
Meeting Exchange
Manage Meeting Exchange and Avaya Aura Conferencing 6.0 elements

Messaging
Manage Avaya Aura Messaging, Communication Manager Messaging, and Modular Messaging

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager



Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Failover Groups
Local Host Name Resolution
Home / Elements / Session Manager / Network Configuration / Local Host Name Resolution-

Local Host Name Resolution

This page allows you to add, edit, or remove local host name entries. Host name entries on this page will override information provided by DNS.

Local Host Name Entries

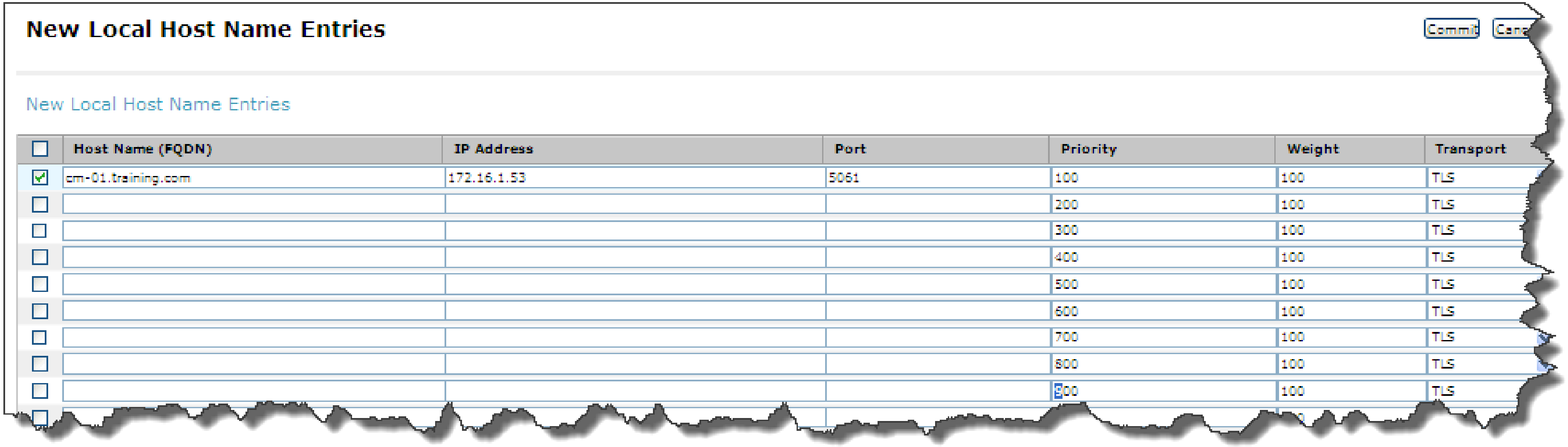
New
Edit
Delete
More Actions ▾
0 Items | Refresh

□	Host Name (FQDN)	IP Address	Port	Priority
	No Local Host Name entries have been defined			

Local Host Name Resolution (continued)

- Enter the FQDN and the IP Address it should resolve to. This is an “internal” DNS lookup table.
- The priority field can be used to setup:

1. Load Balancing – Assign the same priority and weight to all the entries of the same FQDN. You can also assign the same priority but different weights to add more control to the load balancing decision.
2. Failover – Assign different priorities to entries of the same FQDN. The lowest number is the highest priority and would be attempted first.



New Local Host Name Entries

New Local Host Name Entries

□	Host Name (FQDN)	IP Address	Port	Priority	Weight	Transport
☑	cm-01.training.com	172.16.1.53	5061	100	100	TLS
□				200	100	TLS
□				300	100	TLS
□				400	100	TLS
□				500	100	TLS
□				600	100	TLS
□				700	100	TLS
□				800	100	TLS
□				900	100	TLS

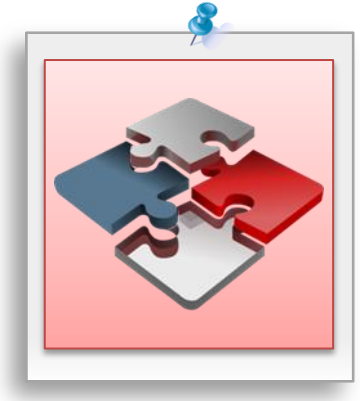
Exercise: Modify SIP Entity for Local Host Name Resolution

Step	Action
1	Navigate to the Routing Menu>>SIP Entities -Modify the SIP Entity for your Partner's Session Manager to an FQDN (use the Classroom Layout PDF)
2	Add an entry in the Local Host Name Resolution to resolve the FQDN to an IP Address
3	Place a call to that destination
4	Commit

Lesson Summary

You have completed the following lesson objectives:

- Examine the use of adaptations and apply adaptations to effect centralized routing between SIP and H.323 endpoints.



Module Summary

You have completed the following lesson objectives:

- SIP Registration/SIP Registry Routing
- Describe Session Manager’s role as a Registrar and in Registry Routing
- Create a SIP User
- Use SIP Tracing Tools
- Examine SIP Registry Routing

NRP

- Review and configure the following routing components to support centralized routing within the enterprise:
  - Domain
  - Location
  - SIP Entities
  - Entity Links
  - Time Ranges
  - Routing Policies
  - Dial Patterns
  - Regular Expressions

Adaptation

- Examine the use of adaptations and apply adaptations to effect centralized routing between SIP and H.323 endpoints.

AVAYA | LEARNING

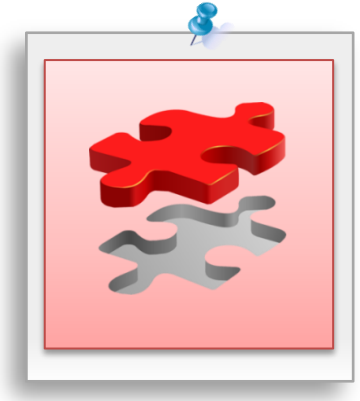
Module 5

Feature Server Application Integration

Module Objectives

After completing this module, you will be able to:

- Identify the role of Session Manager in applying features to calls and administer named and sequenced applications.
- Administer Sequenced Applications.
- Administer features to non-SIP users using Implicit Users.



Lesson 1

Application of Features to Calls – Setting the Scene

Lesson Objectives

After completing this lesson, you will be able to:

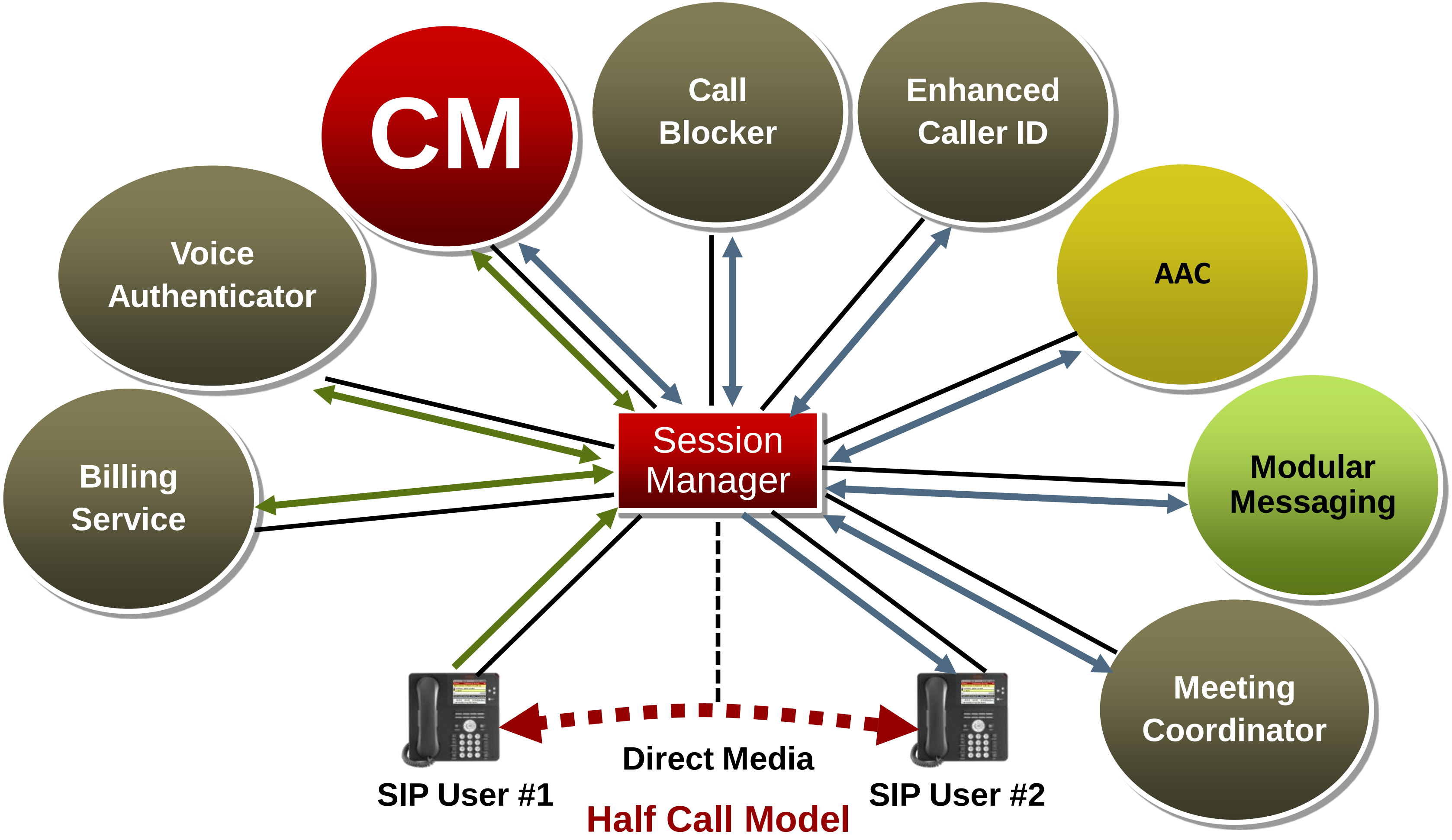
- Review the nature of both named and sequenced applications, and the role of Session Manager in applying such features.

AVAYA | LEARNING

Overview of Applications

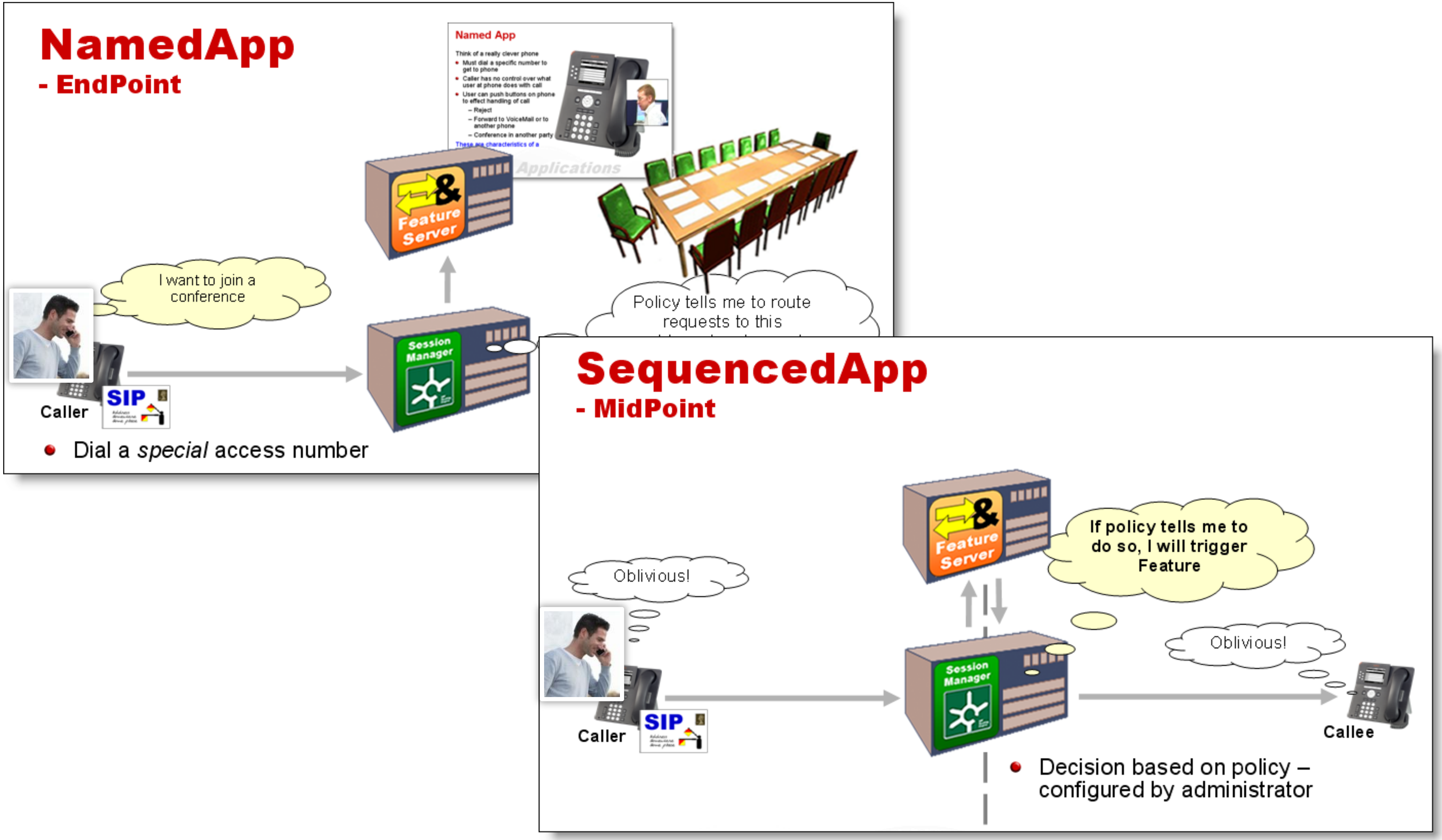
Sequenced & Named Applications

Avaya Aura^{TM} Applications in an IMS Network



Half Call Model

Sequenced and Named Applications



NamedApp

- EndPoint

Named App

Think of a really clever phone

- Must dial a specific number to get to phone
- Caller has no control over what user at phone does with call
- User can push buttons on phone to effect handling of call
  - Reject
  - Forward to VoiceMail or to another phone
  - Conference in another party

These are characteristics of a

Applications
Feature Server
I want to join a conference
Policy tells me to route requests to this
Session Manager
Caller
SIP

- Dial a *special* access number

SequencedApp

- MidPoint

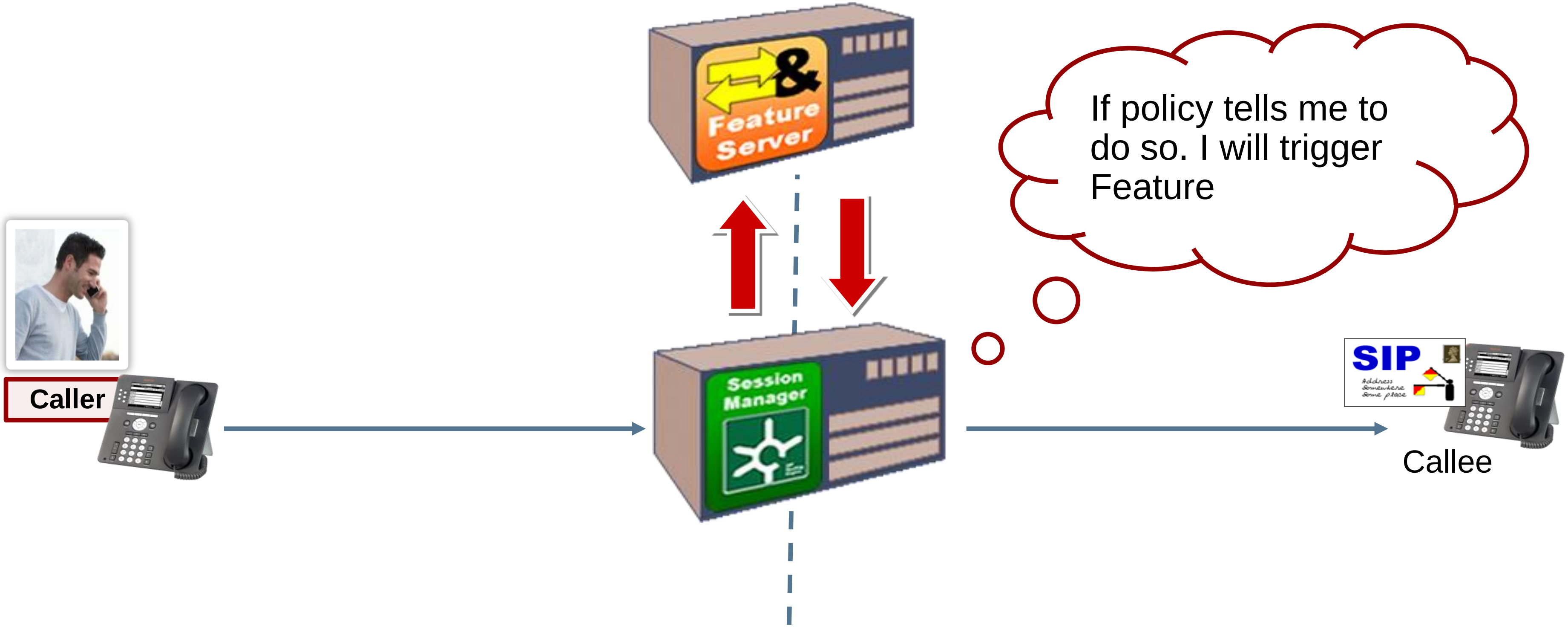
- Decision based on policy – configured by administrator

Sequenced Applications

Named Apps & Sequenced Apps

The difference?

- Decision based on policy – configured by administrator

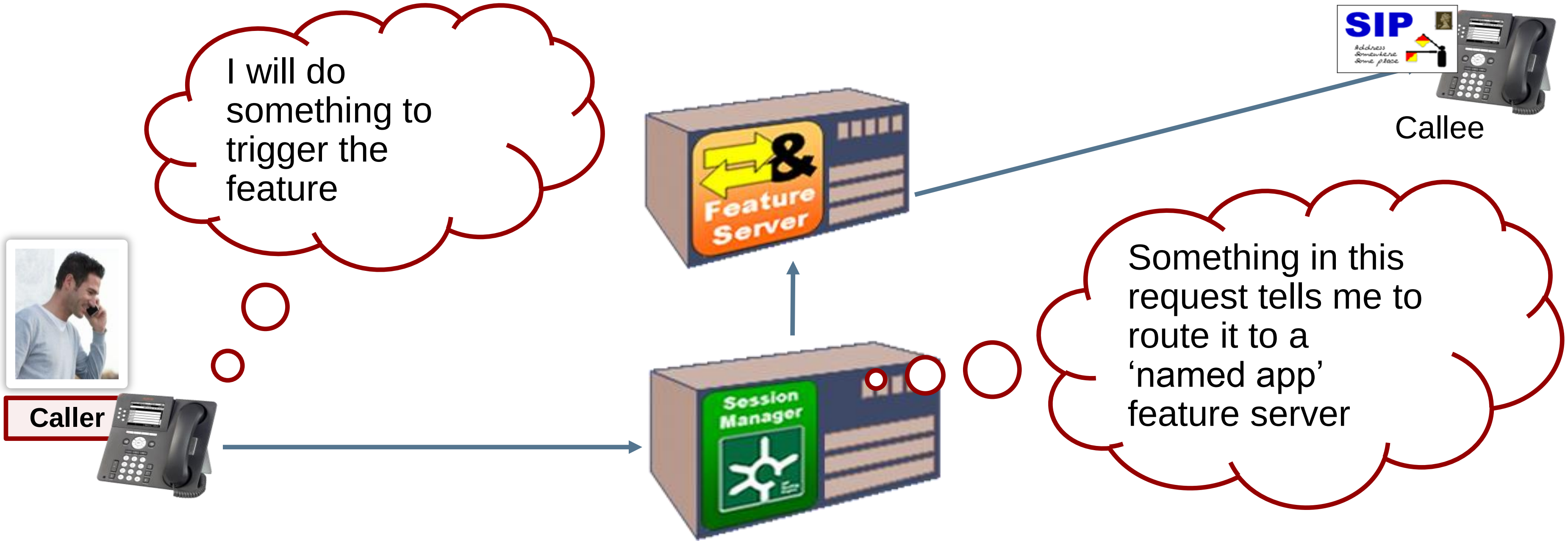


Named Applications

Named Apps & Sequenced Apps

The difference?

- Dial a *special* access number
- Issue a request with *special* details in URI,



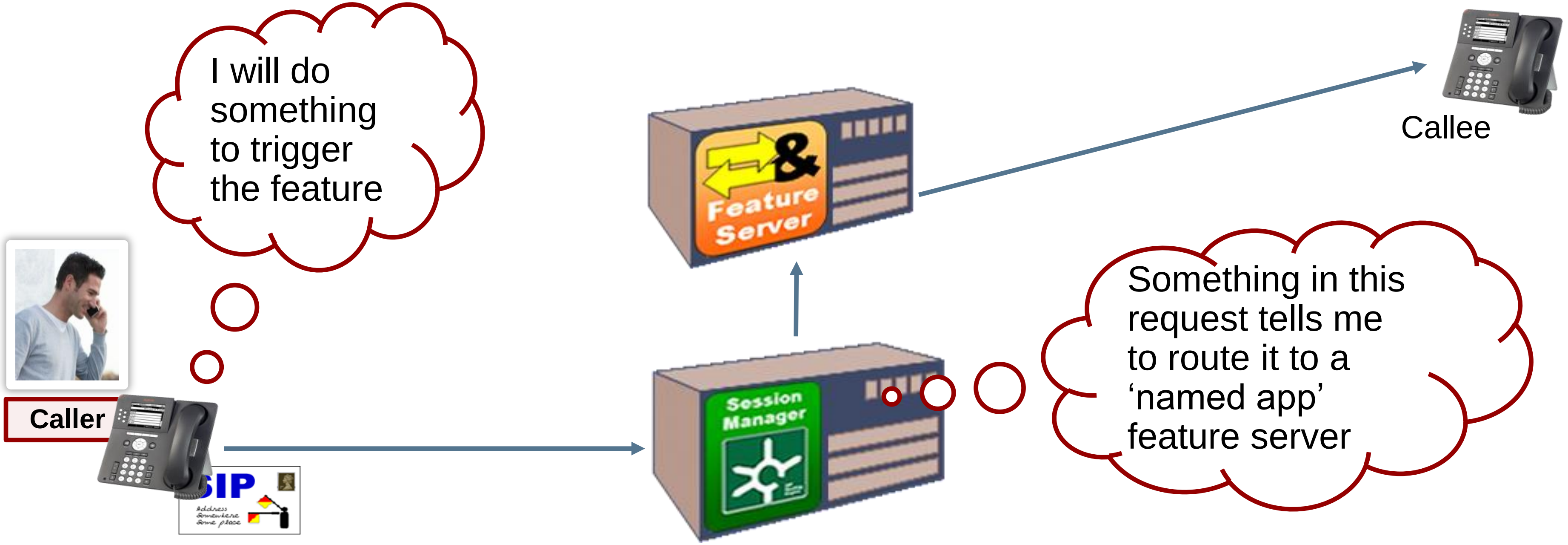
I will do something to trigger the feature

Something in this request tells me to route it to a ‘named app’ feature server

Named Applications

Named Apps & Sequenced Apps the Difference?

- Named Applications



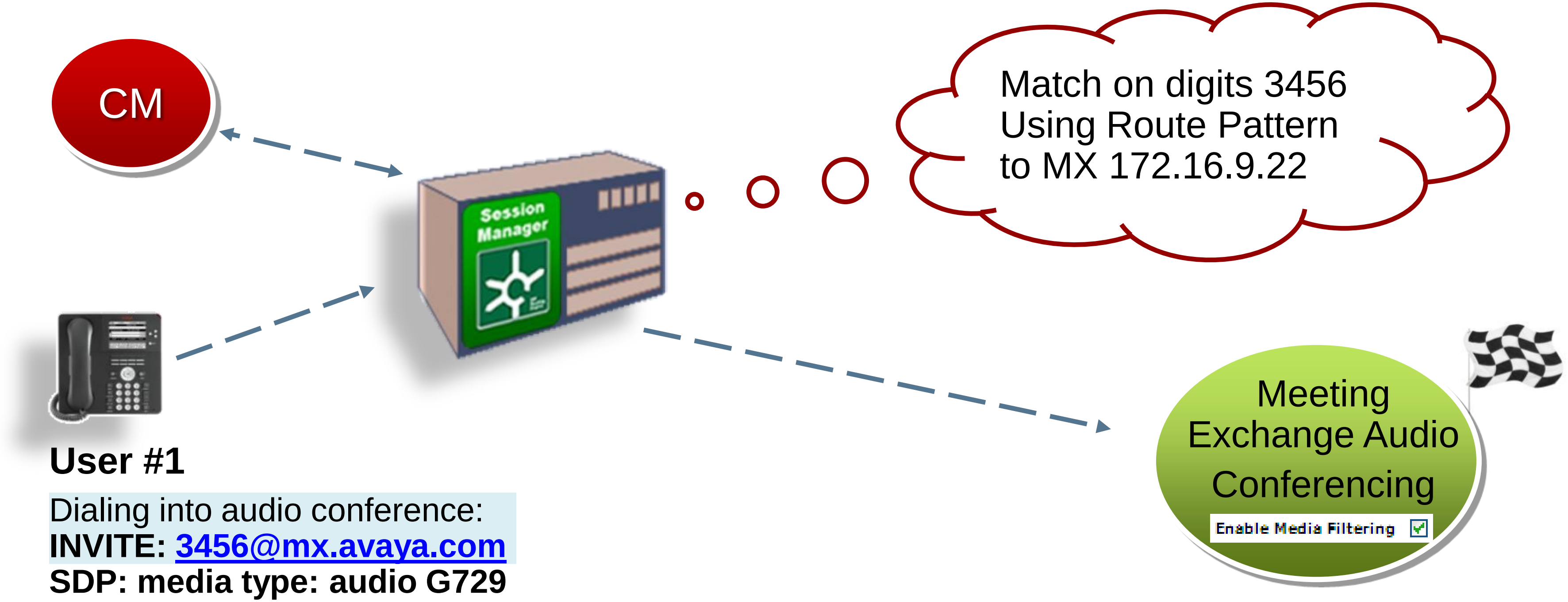
I will do something to trigger the feature

Something in this request tells me to route it to a ‘named app’ feature server

Dial a *special* access number
Issue a request with *special* details in URI.

Named Application

- In Named Applications, the user initiates the call to the application.
- Once dialled, the caller has no control over what happens when the call reaches the application.
- The application can forward the call to voicemail, or to another extension, or could choose to answer the call and bridge it straight in to a conference.
- These are the characteristics of a named application.



CM

Match on digits 3456
Using Route Pattern
to MX 172.16.9.22

Meeting Exchange Audio Conferencing

Enable Media Filtering ☑

User #1

Dialing into audio conference:
INVITE: 3456@mx.avaya.com
SDP: media type: audio G729

Named Application Routing

Named Applications are NOT sequenced

Two possible ways to route to Named Application:

- Routing Policy

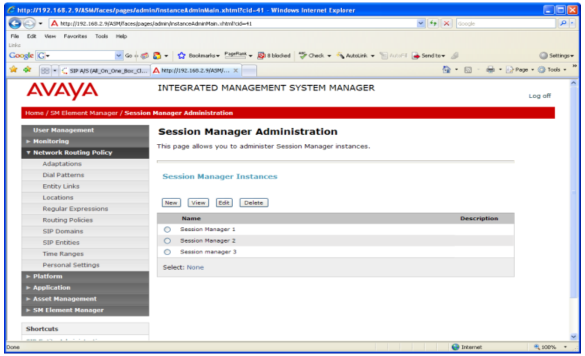
- Register Application as SIP User

SIP Location

Creating Network Routing Policies

- Basically, you create routing policies to route calls to a NAME APP.

Network Administrator



http://192.168.2.9/ASM/faces/pages/admin/instanceAdminMain.xhtml?cid=41 - Windows Internet Explorer
http://192.168.2.9/ASM/faces/pages/admin/instanceAdminMain.xhtml?cid=41
File Edit View Favorites Tools Help
Links
Google
Go
Bookmarks
PageRank
8 blocked
Check
AutoLink
AutoFill
Send to
Settings
SIP A/S (All_On_One_Box_Cl...
http://192.168.2.9/ASM/...
Page
Tools
AVAYA
INTEGRATED MANAGEMENT SYSTEM MANAGER
Log off
Home / SM Element Manager / Session Manager Administration
User Management
Monitoring
Network Routing Policy
Adaptations
Dial Patterns
Entity Links
Locations
Regular Expressions
Routing Policies
SIP Domains
SIP Entities
Time Ranges
Personal Settings
Platform
Application
Asset Management
SM Element Manager
Shortcuts
Done
Internet
100%

Session Manager Administration

This page allows you to administer Session Manager instances.

Session Manager Instances

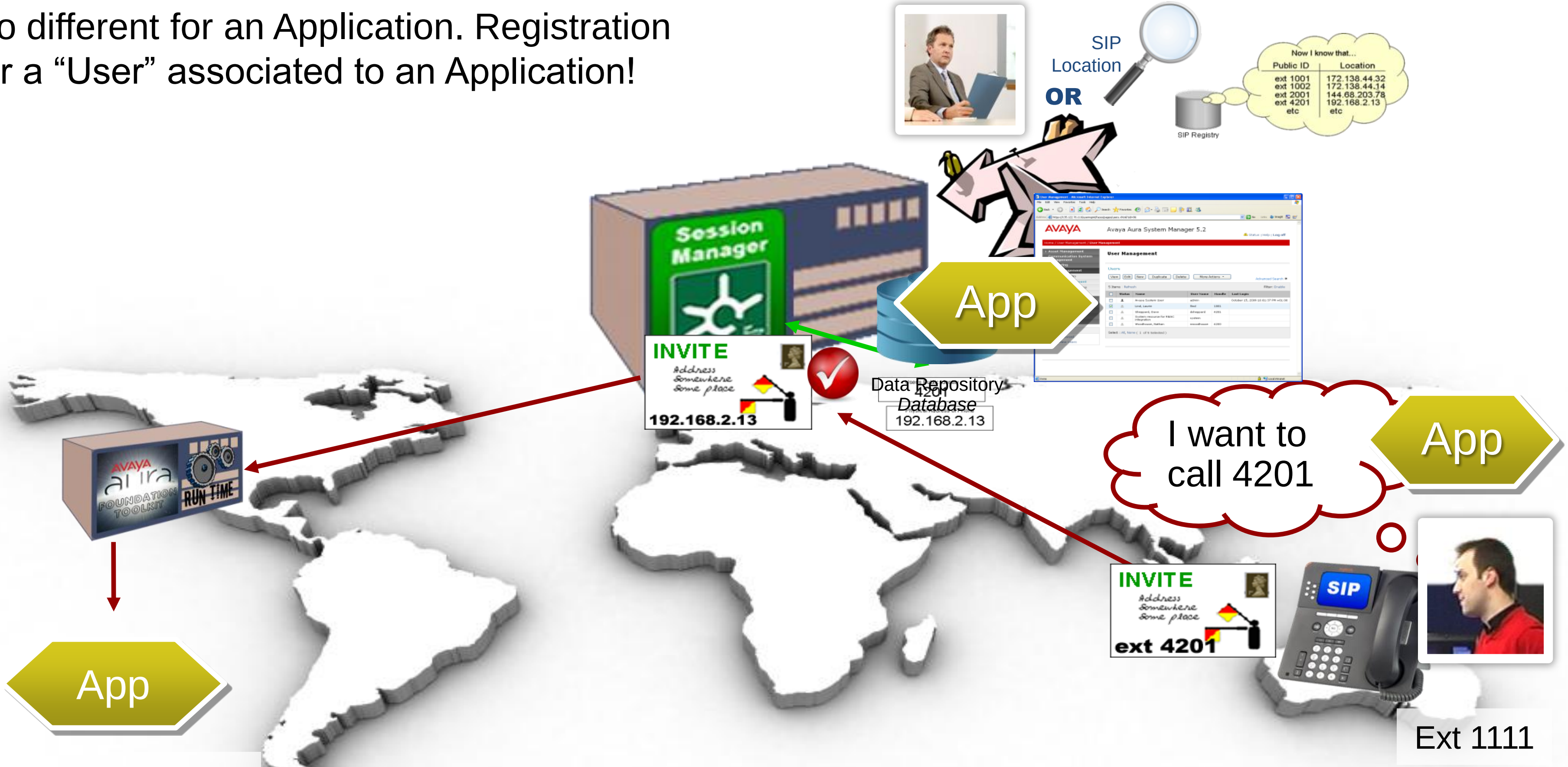
New | View | Edit | Delete

	Name	Description
○	Session Manager 1	
○	Session Manager 2	
○	Session manager 3	

Select: None

Named App as SIP User

No different for an Application. Registration for a "User" associated to an Application!



Application Registers as 4201

SIP Registry

Session Manager checks for User Profile

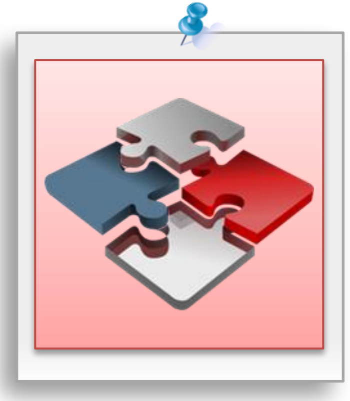
If profile exists, checks registry for registration

If registered get destination location from registry and proxy on

Lesson Summary

You have completing the following lesson objective:

- Review the nature of both named and sequenced applications, and the role of Session Manager in applying such features.



AVAYA | LEARNING

Lesson 2 Administering Sequenced Applications

Feature Servers

Lesson Objectives

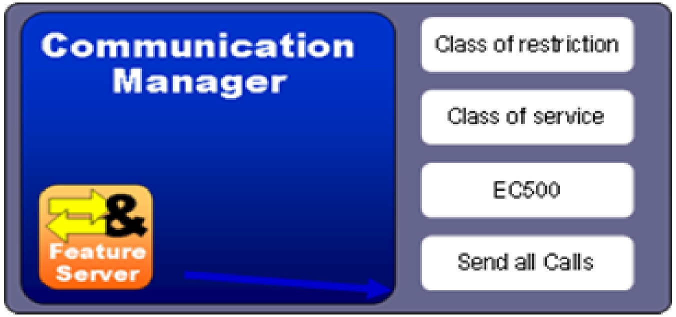
After completing this lesson, you will be able to:

- Review the nature of sequenced applications, and how they are administered.

Benefit of Application Sequencing

- Session Manager watches over Registered SIP Users and all of their calls, both incoming and outgoing, ready to take any special action when the occasion requires.

CM Feature Server as a Sequenced Application

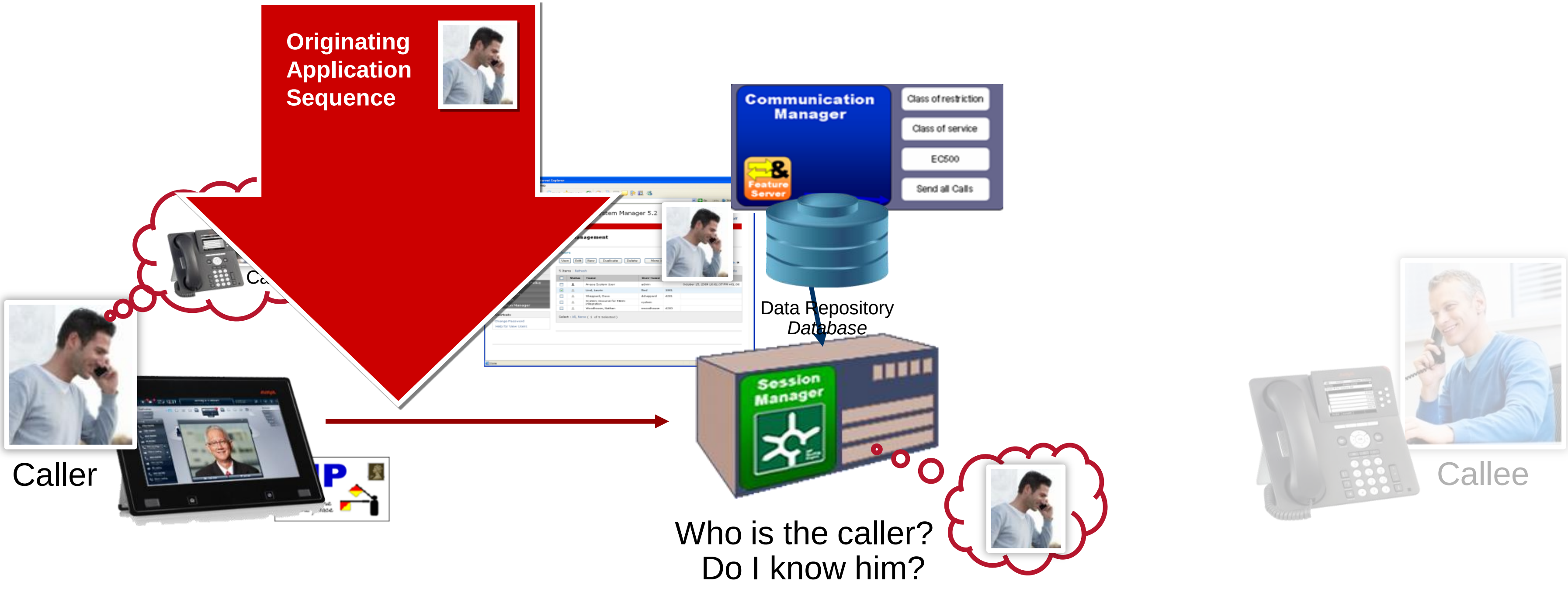


CM has thousands of “features”. Since the CM has knowledge of the user, the Session Manager does not have to address each feature.

It simply sends the request to CM and CM will apply the appropriate features based on the user and whether they are the caller or the callee.

How CM Features are Applied

- Session Manager retrieves caller’s User Profile
- Retrieves callers Originating Application Sequence
- An ordered list of applications to be applied to outbound calls made by the caller

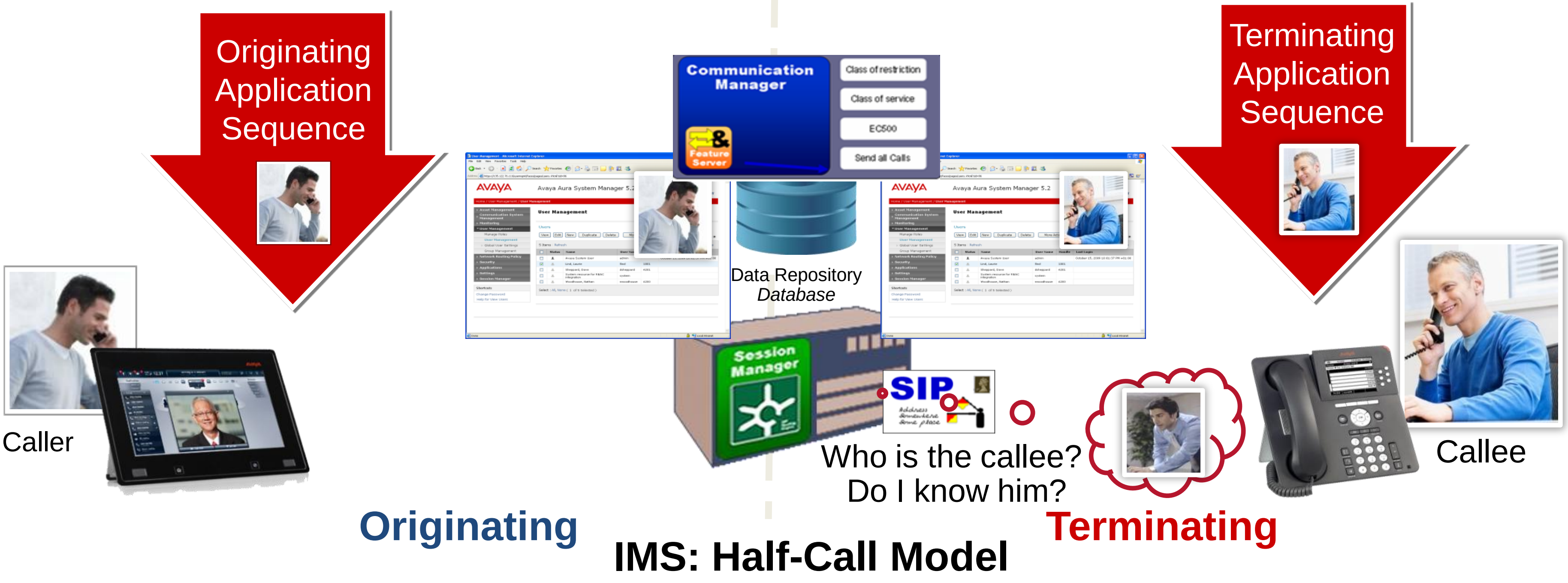


IMS: Half-Call Model

Half Call Model

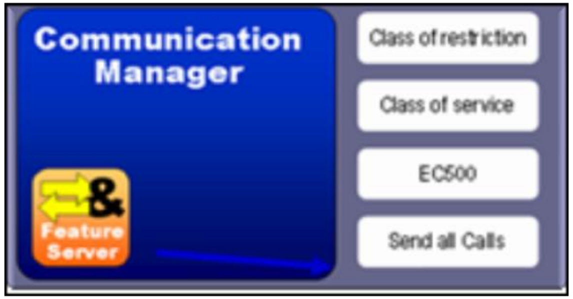
- Session Manager retrieves caller’s UserProfile
- Retrieves callers Originating Application Sequence
  - An ordered list of applications to be applied to outbound calls made by the caller

- Session Manager retrieves callee’s UserProfile
- Retrieves callees Terminating Application Sequence
  - An ordered list of applications to be applied to inbound calls made by the callee



CM Relationships to ASM and Order of Implementation

1. SIP Entity
2. Managed Element
3. Application
4. Added to Application Sequence



Note

CM must be added to Session Manager as a Managed Element first before it can be created as an Application.

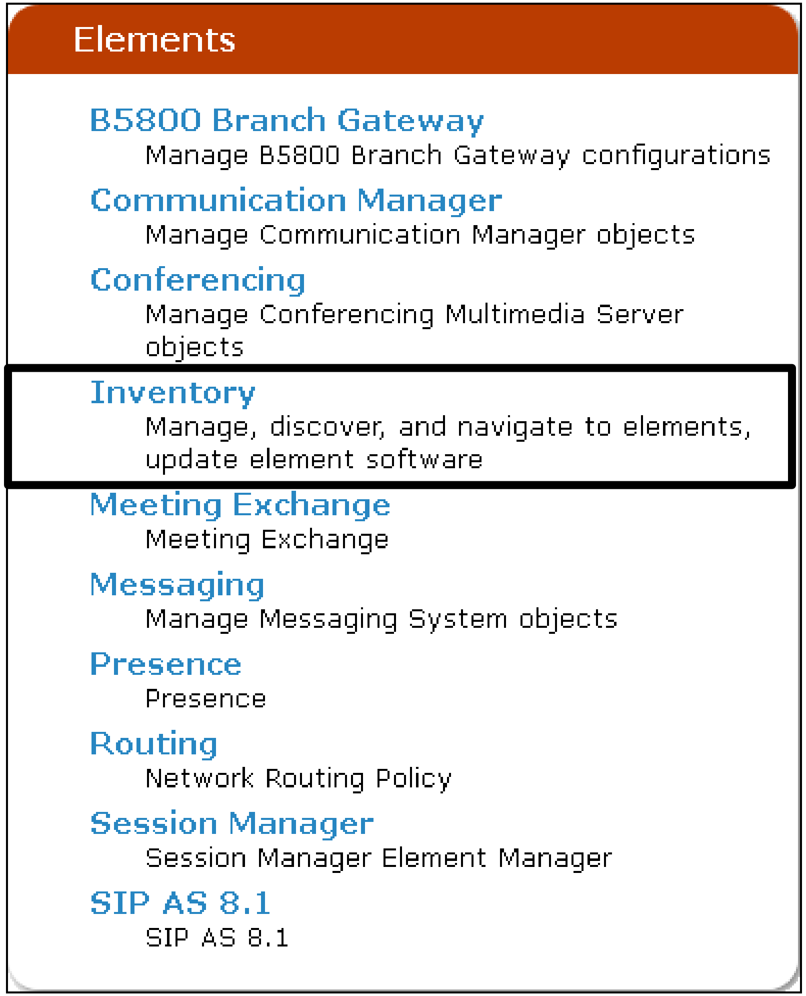
AVAYA | LEARNING

Communication Manager as a Managed Element

Communication System Manager

The *Communication System Manager* interface can be used to synchronize CM station data to the System Manager database.

From the SMGR web console select **Inventory.**



Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway configurations

Communication Manager
Manage Communication Manager objects

Conferencing
Manage Conferencing Multimedia Server objects

Inventory
Manage, discover, and navigate to elements, update element software

Meeting Exchange
Meeting Exchange

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

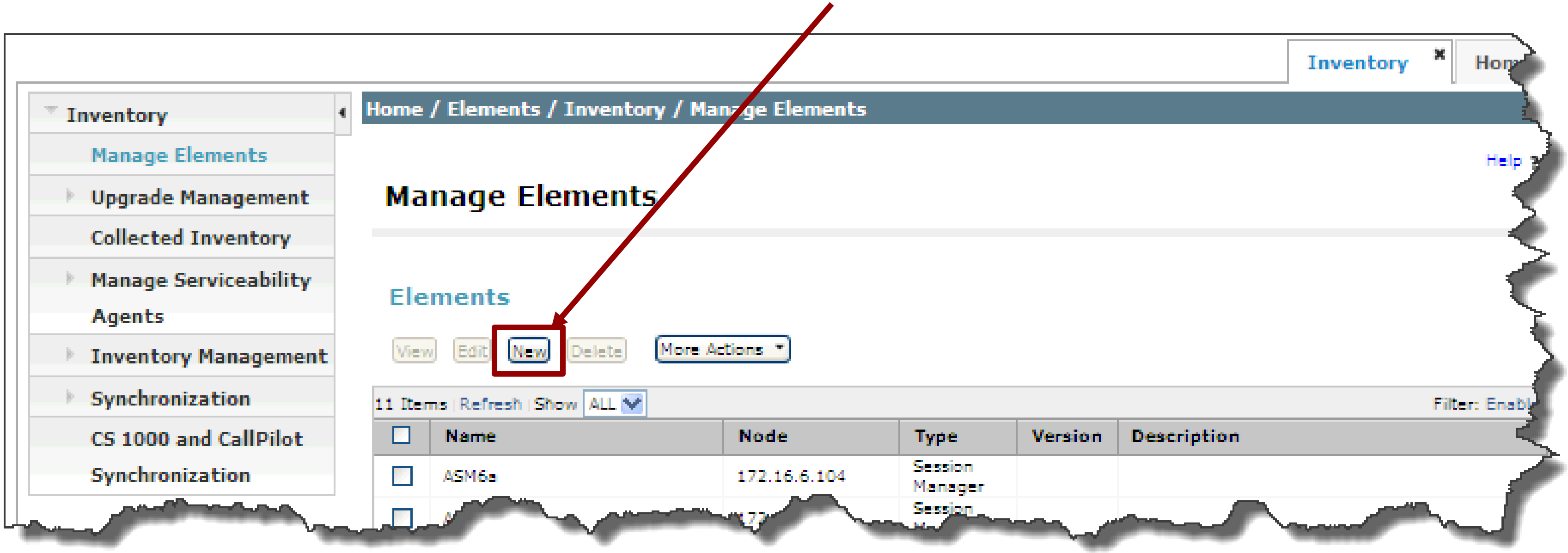
Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Communication System Manager (continued)

The *Communication System Manager* interface can be used to synchronize CM station data to the System Manager database.

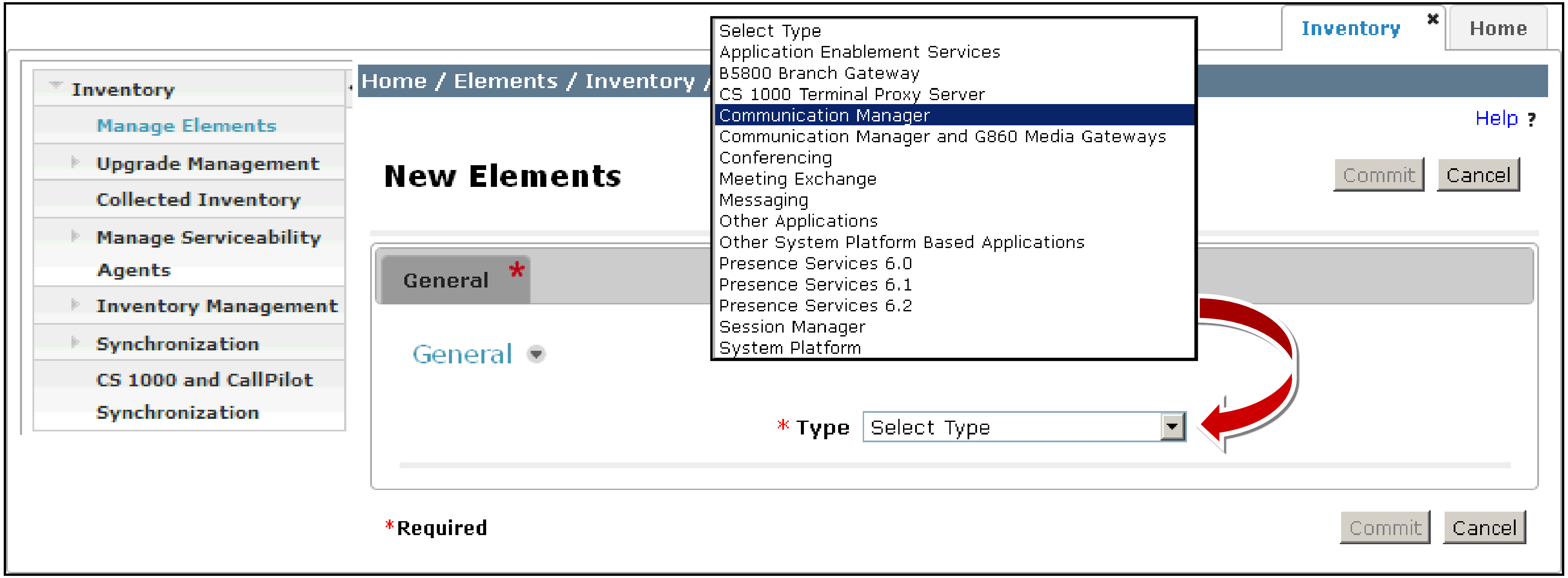
To create CM as a Managed Element Select **New**



□	Name	Node	Type	Version	Description
□	ASM6s	172.16.6.104	Session Manager		

Communication System Manager (continued)

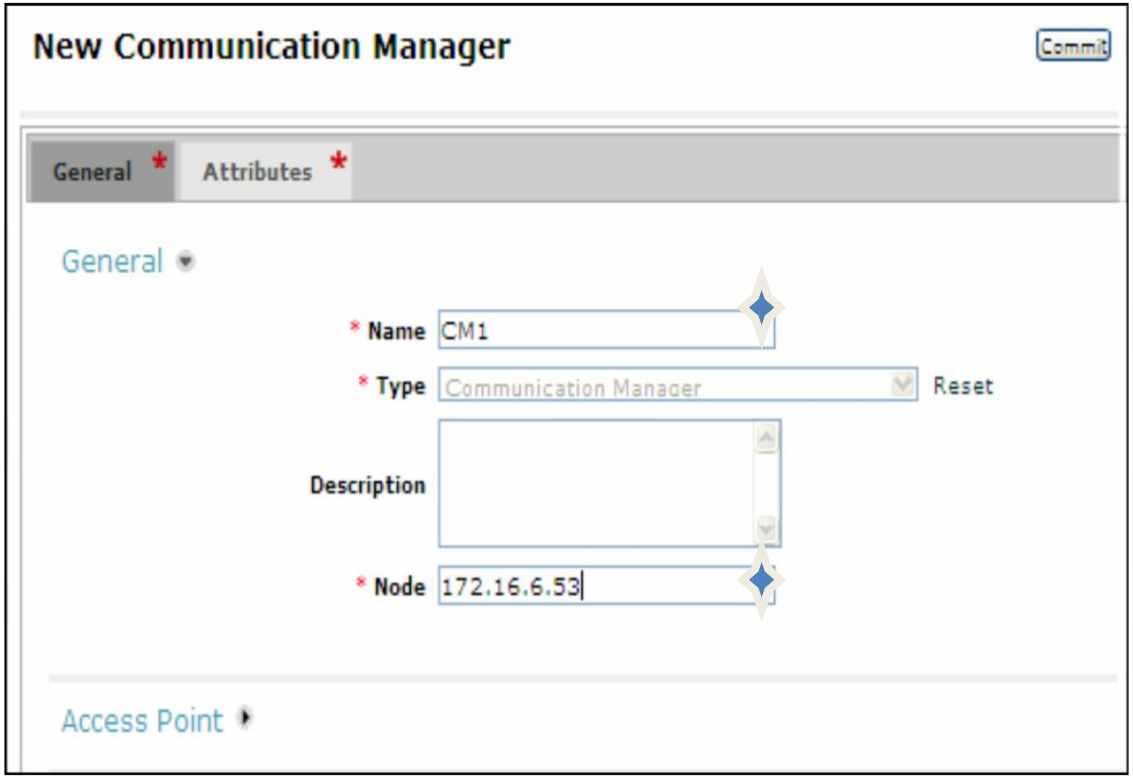
Select the Communication Manager “Type” from the drop-down list.



Select Type
Application Enablement Services
B5800 Branch Gateway
CS 1000 Terminal Proxy Server
Communication Manager
Communication Manager and G860 Media Gateways
Conferencing
Meeting Exchange
Messaging
Other Applications
Other System Platform Based Applications
Presence Services 6.0
Presence Services 6.1
Presence Services 6.2
Session Manager
System Platform

Communication System Manager (continued)

Specify the name and IP address of the Communication Manager 172.16.x.53.



New Communication Manager

* Name: CM1

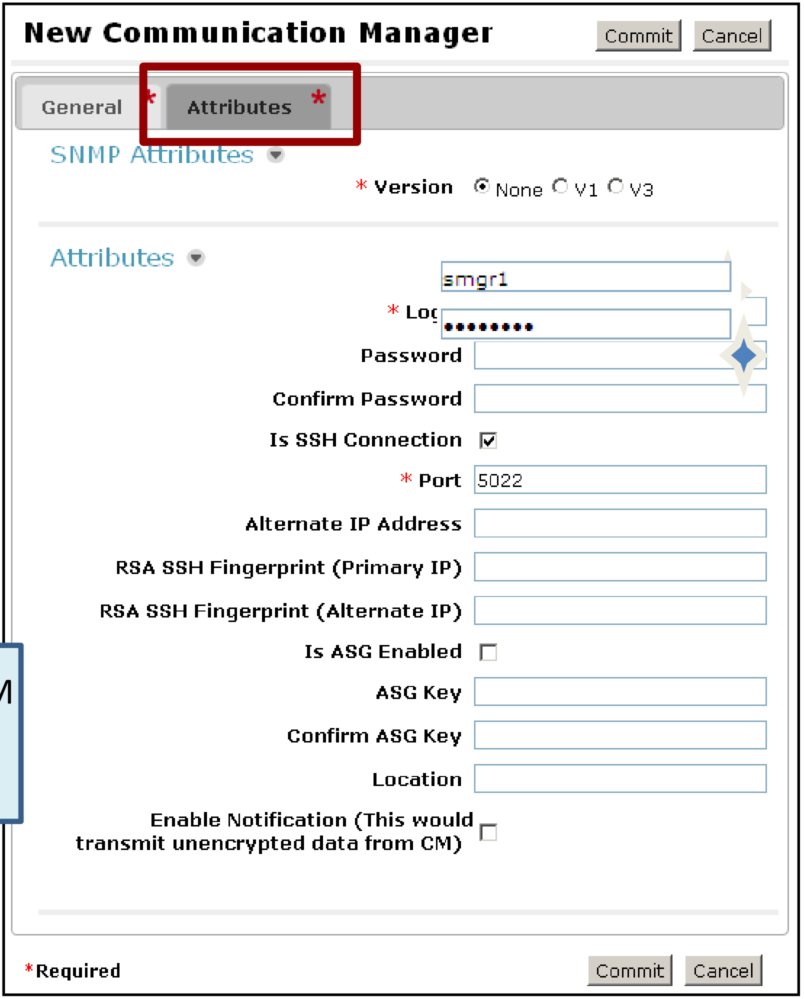
* Type: Communication Manager

Description:

* Node: 172.16.6.53

Communication System Manager (continued)

The login used must have ssh/sat access to Communication Manager.



New Communication Manager Commit Cancel

General * | Attributes *

SNMP Attributes

* Version ● None ○ V1 ○ V3

Attributes

smgr1

* Log ••••••••

Password

Confirm Password

Is SSH Connection ☑

* Port 5022

Alternate IP Address

RSA SSH Fingerprint (Primary IP)

RSA SSH Fingerprint (Alternate IP)

Is ASG Enabled □

ASG Key

Confirm ASG Key

Location

Enable Notification (This would transmit unencrypted data from CM) □

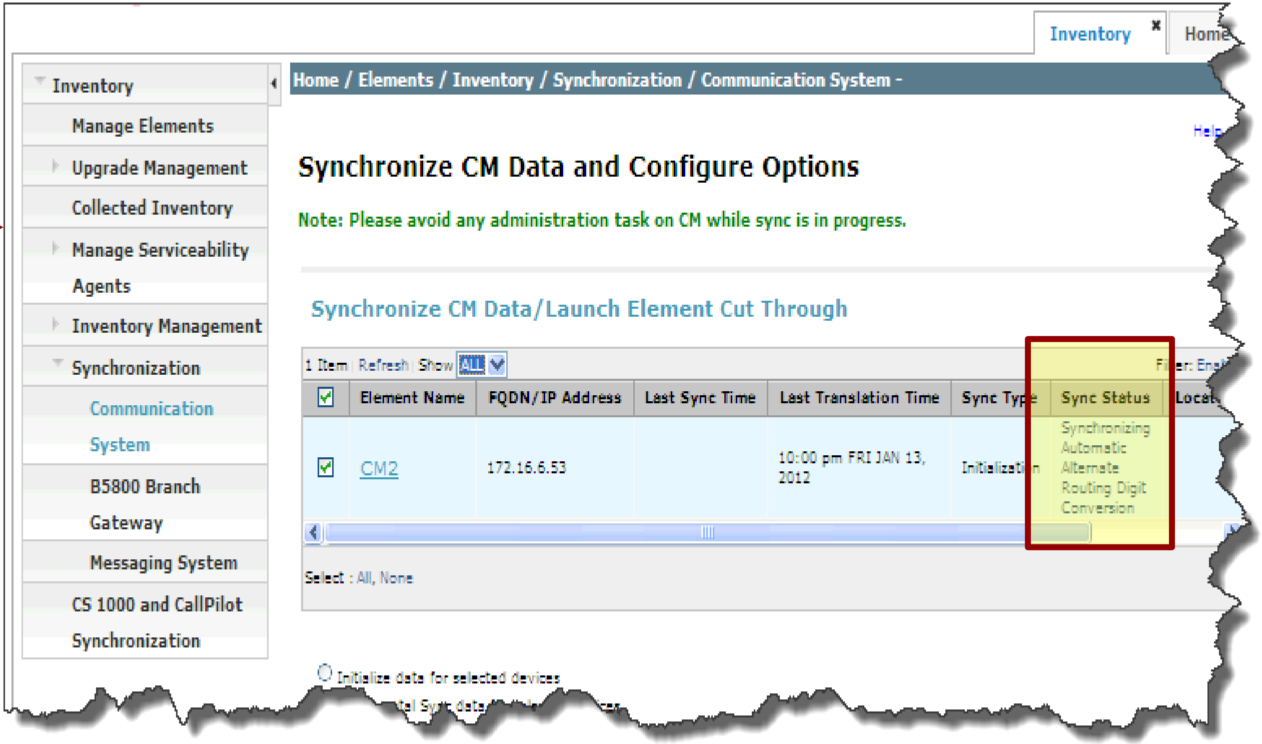
*Required Commit Cancel

Do not use any of the following logins when administering a CM entity for Communication System Manager:
craft, craft2, admin, inads, init, rasaccess, sroot, and tsc

Scheduling CM Data Synchronization

As soon as the element is saved, the initial sync is performed.

To view, navigate to **Synchronization >> Communication System**



Synchronize CM Data and Configure Options

Note: Please avoid any administration task on CM while sync is in progress.

Synchronize CM Data/Launch Element Cut Through

☑	Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type	Sync Status	Locat
☑	CM2	172.16.6.53		10:00 pm FRI JAN 13, 2012	Initialization	Synchronizing Automatic Alternate Routing Digit Conversion	

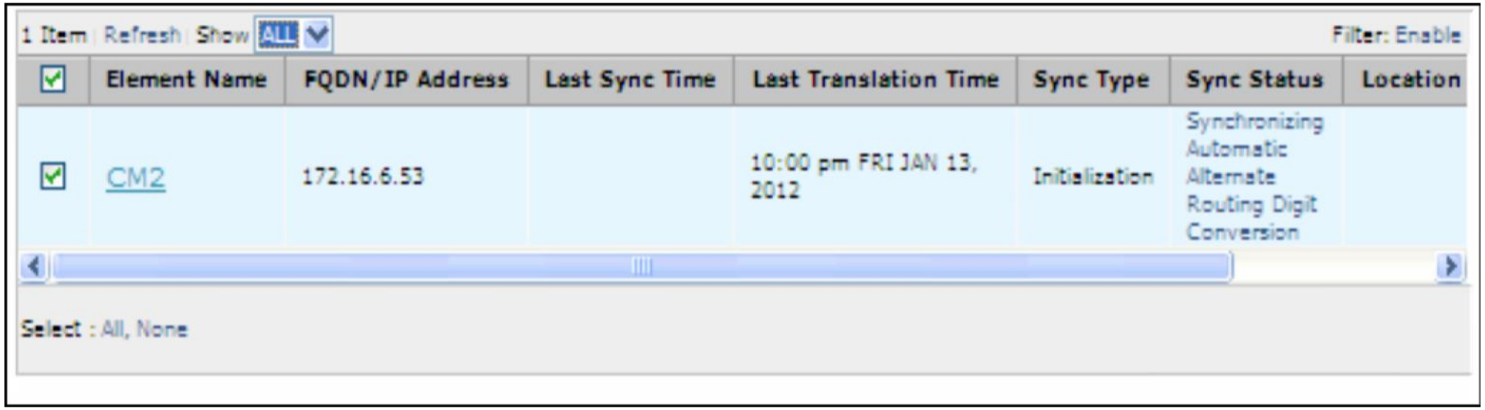
○ Initialize data for selected devices

tal Sync data

Element Manager – Data Synchronization

Automatic CM Data Synchronization

- After a CM has been added as a Managed Element, it will be automatically scheduled for an initial and subsequent incremental data synchronization.
  - Subsequent changes made in System Manager will immediately update underlying CM when committed.
  - **In 6.2 Synchronization enhancements include almost immediate synchronization from CM to SMGR.**



1 Item | Refresh | Show ALL

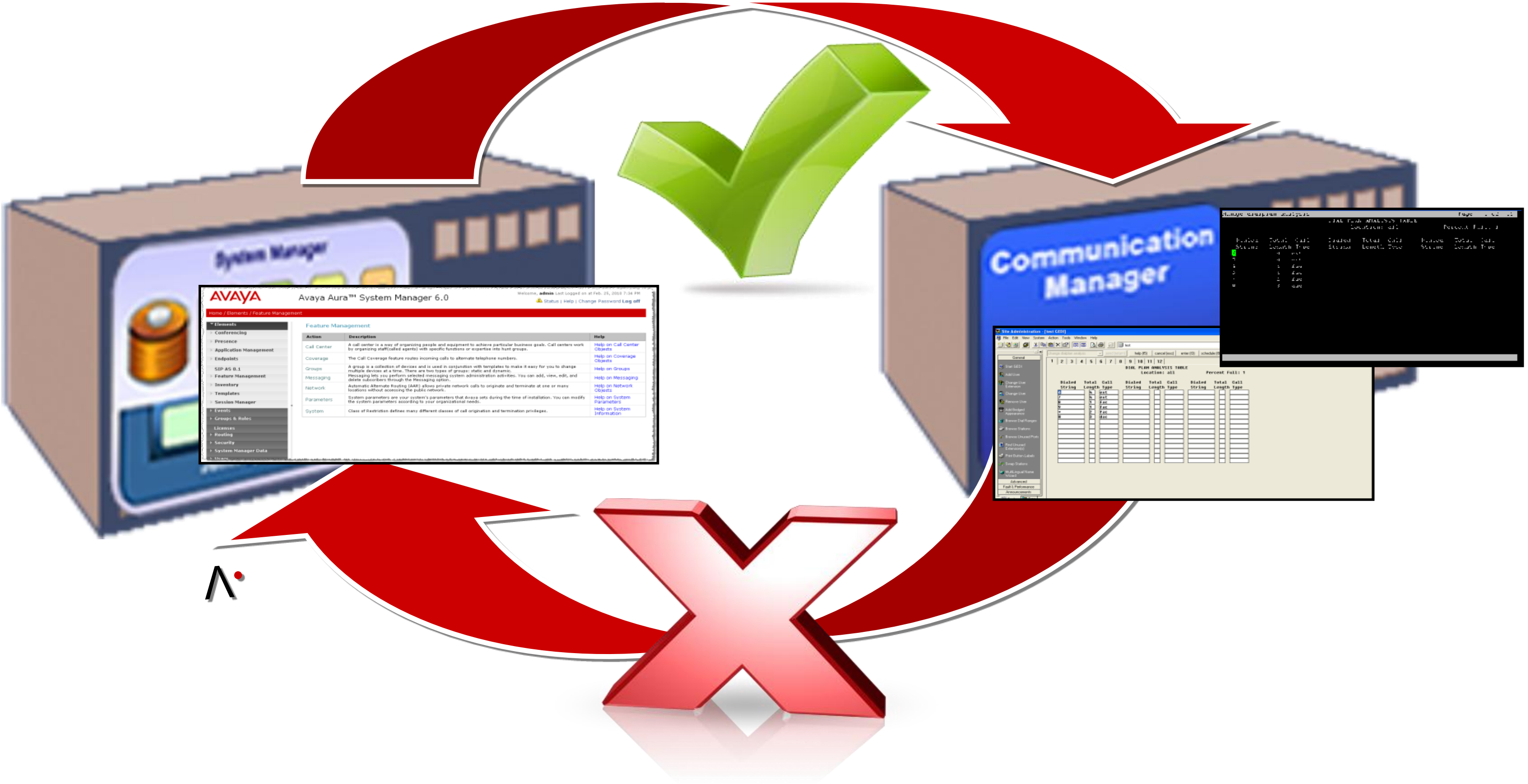
Filter: Enable

☑	Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type	Sync Status	Location
☑	CM2	172.16.6.53		10:00 pm FRI JAN 13, 2012	Initialization	Synchronizing Automatic Alternate Routing Digit Conversion	

Select : All, None

Making Changes to Data – 6.1

- Subsequent changes made in System Manager will immediately update the underlying CM when committed.
- In 6.1 if subsequent changes were made in the CM, they would not be reflected in SMGR until the next scheduled synchronization.



Feature Management

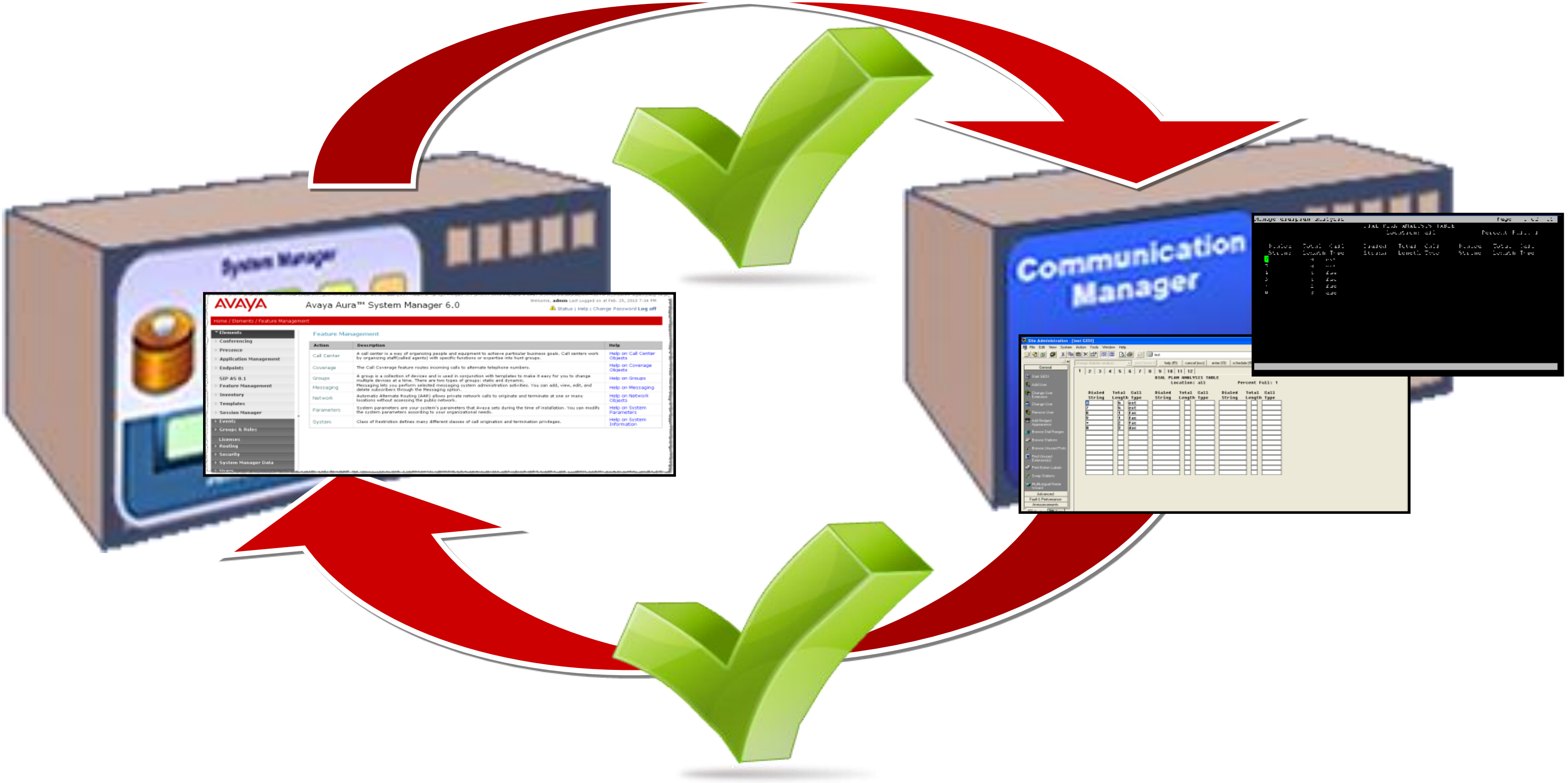
Action	Description	Help
Call Center	A call center is a way of organizing people and equipment to achieve particular business goals. Call centers work by organizing staff(called agents) with specific functions or expertise into hunt groups.	Help on Call Center Objects
Coverage	The Call Coverage feature routes incoming calls to alternate telephone numbers.	Help on Coverage Objects
Groups	A group is a collection of devices and is used in conjunction with templates to make it easy for you to change multiple devices at a time. There are two types of groups: static and dynamic.	Help on Groups
Messaging	Messaging lets you perform selected messaging system administration activities. You can add, view, edit, and delete subscribers through the Messaging option.	Help on Messaging
Network	Automatic Alternate Routing (AAR) allows private network calls to originate and terminate at one or many locations without accessing the public network.	Help on Network Objects
Parameters	System parameters are your system's parameters that Avaya sets during the time of installation. You can modify the system parameters according to your organizational needs.	Help on System Parameters
System	Class of Restriction defines many different classes of call origination and termination privileges.	Help on System Information

DIAL PLAN ANALYSIS TABLE
Location: all   Percent Full: 1

Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
6	4	ext						
7	4	ext						
8	1	fac						
9	1	fac						
*	2	fac						
#	3	dac						

Making Changes to Data – 6.2

- Since 6.2, changes made in CM will be reflected in System Manager almost immediately!

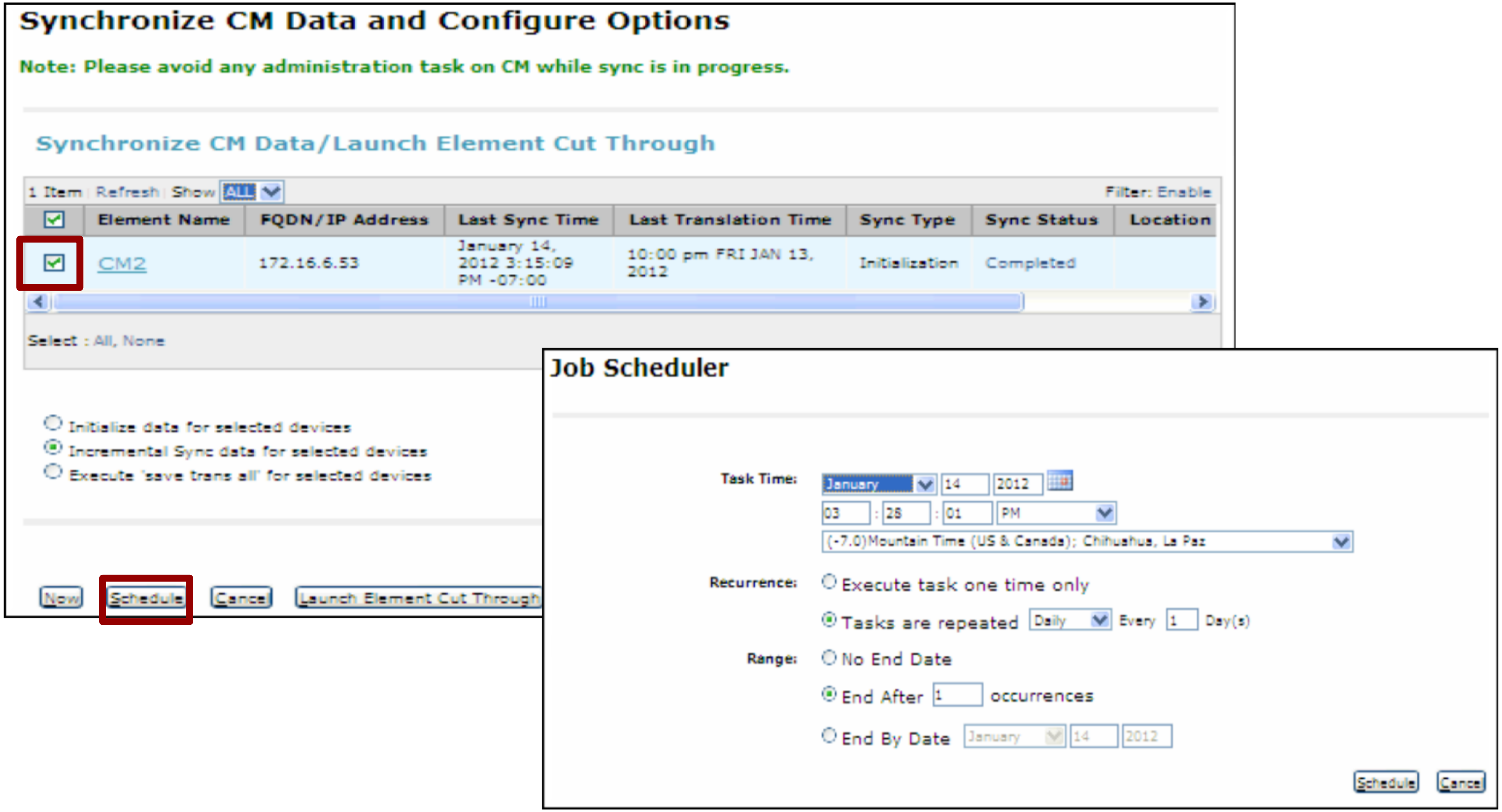


Feature Management

Action	Description	Help
Call Center	A call center is a way of organizing people and equipment to achieve particular business goals. Call centers work by organizing staff(called agents) with specific functions or expertise into hunt groups.	Help on Call Center Objects
Coverage	The Call Coverage feature routes incoming calls to alternate telephone numbers.	Help on Coverage Objects
Groups	A group is a collection of devices and is used in conjunction with templates to make it easy for you to change multiple devices at a time. There are two types of groups: static and dynamic.	Help on Groups
Messaging	Messaging lets you perform selected messaging system administration activities. You can add, view, edit, and delete subscribers through the Messaging option.	Help on Messaging
Network	Automatic Alternate Routing (AAR) allows private network calls to originate and terminate at one or many locations without accessing the public network.	Help on Network Objects
Parameters	System parameters are your system's parameters that Avaya sets during the time of installation. You can modify the system parameters according to your organizational needs.	Help on System Parameters
System	Class of Restriction defines many different classes of call origination and termination privileges.	Help on System Information

Scheduling CM Data Synchronization

The CM sync copies the XLN (translation) file from the copy saved on the CM's hard disk to the SMGR database.



Synchronize CM Data and Configure Options

Note: Please avoid any administration task on CM while sync is in progress.

Synchronize CM Data/Launch Element Cut Through

1 Item | Refresh | Show ALL | Filter: Enable

☑	Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type	Sync Status	Location
☑	CM2	172.16.6.53	January 14, 2012 3:15:09 PM -07:00	10:00 pm FRI JAN 13, 2012	Initialization	Completed	

Select : All, None

○ Initialize data for selected devices
● Incremental Sync data for selected devices
○ Execute 'save trans all' for selected devices

Job Scheduler

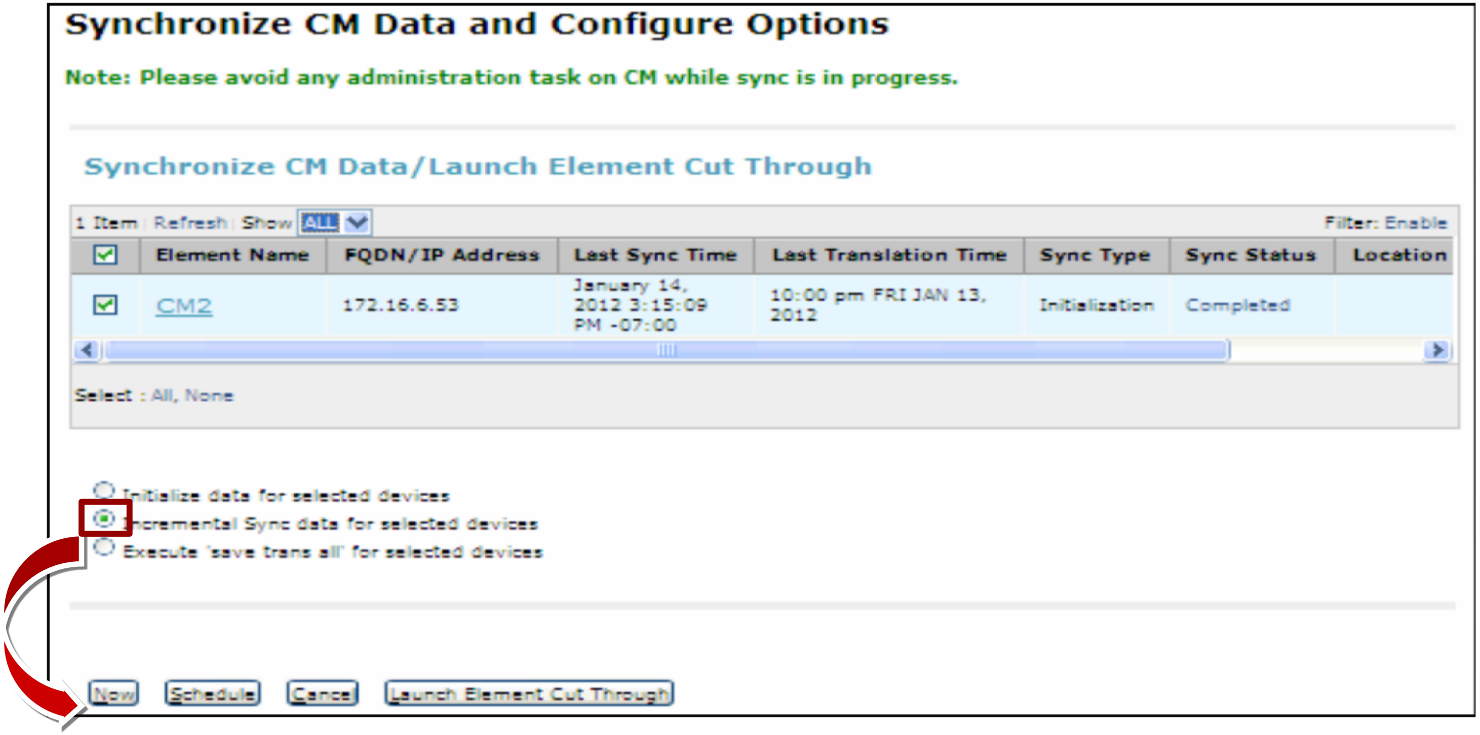
Task Time: January 14 2012
03 : 28 : 01 PM
(-7.0)Mountain Time (US & Canada); Chihuahua, La Paz

Recurrence: ○ Execute task one time only
● Tasks are repeated Daily Every 1 Day(s)

Range: ○ No End Date
● End After 1 occurrences
○ End By Date January 14 2012

Manual CM Data Synchronization

- On the Inventory, Synchronization >> Communication System page, you can select your CM and select the radio button to perform an incremental sync and click now.
- When you modify CM data in System Manager, it is automatically replicated to CM when you select commit.



Synchronize CM Data and Configure Options

Note: Please avoid any administration task on CM while sync is in progress.

Synchronize CM Data/Launch Element Cut Through

☑	Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type	Sync Status	Location
☑	CM2	172.16.6.53	January 14, 2012 3:15:09 PM -07:00	10:00 pm FRI JAN 13, 2012	Initialization	Completed	

Select : All, None

○ Initialize data for selected devices
● Incremental Sync data for selected devices
○ Execute 'save trans all' for selected devices

Exercise: Add CM as a Managed Element

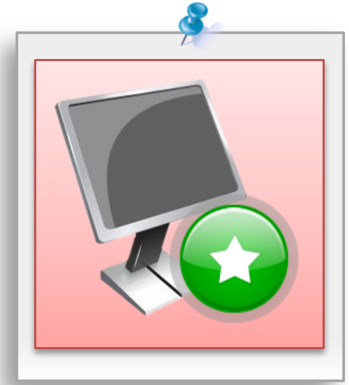
Step	Action
1	At System Manager console select Inventory>>Manage Elements
2	Select **New**
3	Name: CMx or CMx **Pod 1**: CM1; **Pod 2**: CM2; **Pod 3**: CM3; **Pod 4**: CM4; **Pod 5**: CM5; **Pod 6**: CM6
4	Node: 172.16.x.53
5	Login/Password: **Pod 1**: CM1, smgr1/ Passw0rd; **Pod 2**: CM2, smgr2/ Passw0rd; **Pod 3**: CM1, smgr3/ Passw0rd; **Pod 4**: CM2, smgr4/ Passw0rd; **Pod 5**: CM1, smgr5/ Passw0rd; **Pod 6**: CM2, smgr6/ Passw0rd
6	Commit your changes

Step 3 – Name:

Pod 1	**Pod 2**	**Pod 3**	**Pod 4**	**Pod 5**	**Pod 6**
CM1	CM2	CM3	CM4	CM5	CM6

Step 5 – Login/Password:

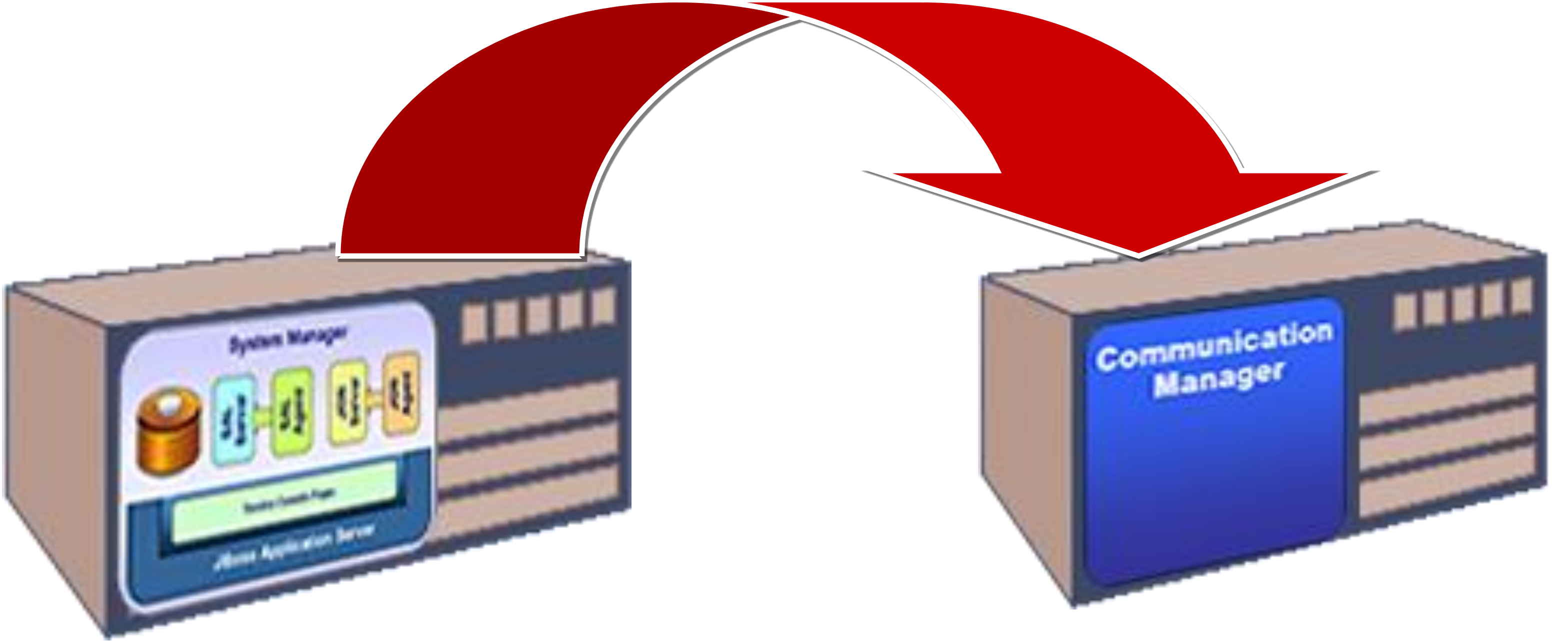
Pod 1	**Pod 2**	**Pod 3**	**Pod 4**	**Pod 5**	**Pod 6**
CM1	CM2	CM1	CM2	CM1	CM2
smgr1/ Passw0rd	smgr2/ Passw0rd	smgr3/ Passw0rd	smgr4/ Passw0rd	smgr5/ Passw0rd	smgr6/ Passw0rd



This exercise requires shadowing to be setup between students as one student will complete the exercise and the other student shadows.

Exercise: View Synchronization Status

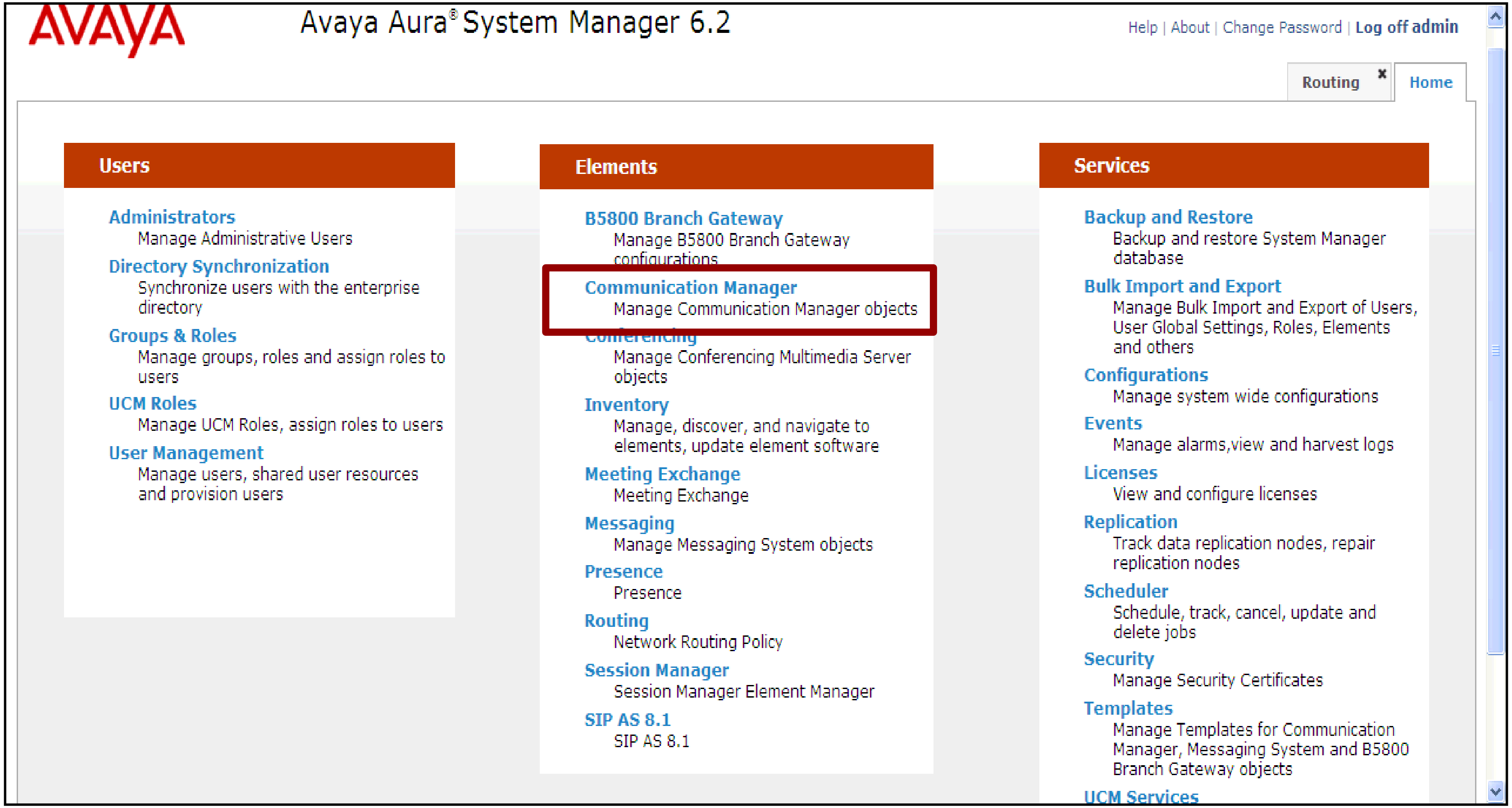
Step	Action
1	Navigate to Inventory >> Synchronization >> Communication System
2	View the Synchronization Status



AVAYA | LEARNING

Viewing Communication Manager Data

Communication Manager



Avaya Aura® System Manager 6.2

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

UCM Roles
Manage UCM Roles, assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway configurations

Communication Manager
Manage Communication Manager objects

Conferencing
Manage Conferencing Multimedia Server objects

Inventory
Manage, discover, and navigate to elements, update element software

Meeting Exchange
Meeting Exchange

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

Scheduler
Schedule, track, cancel, update and delete jobs

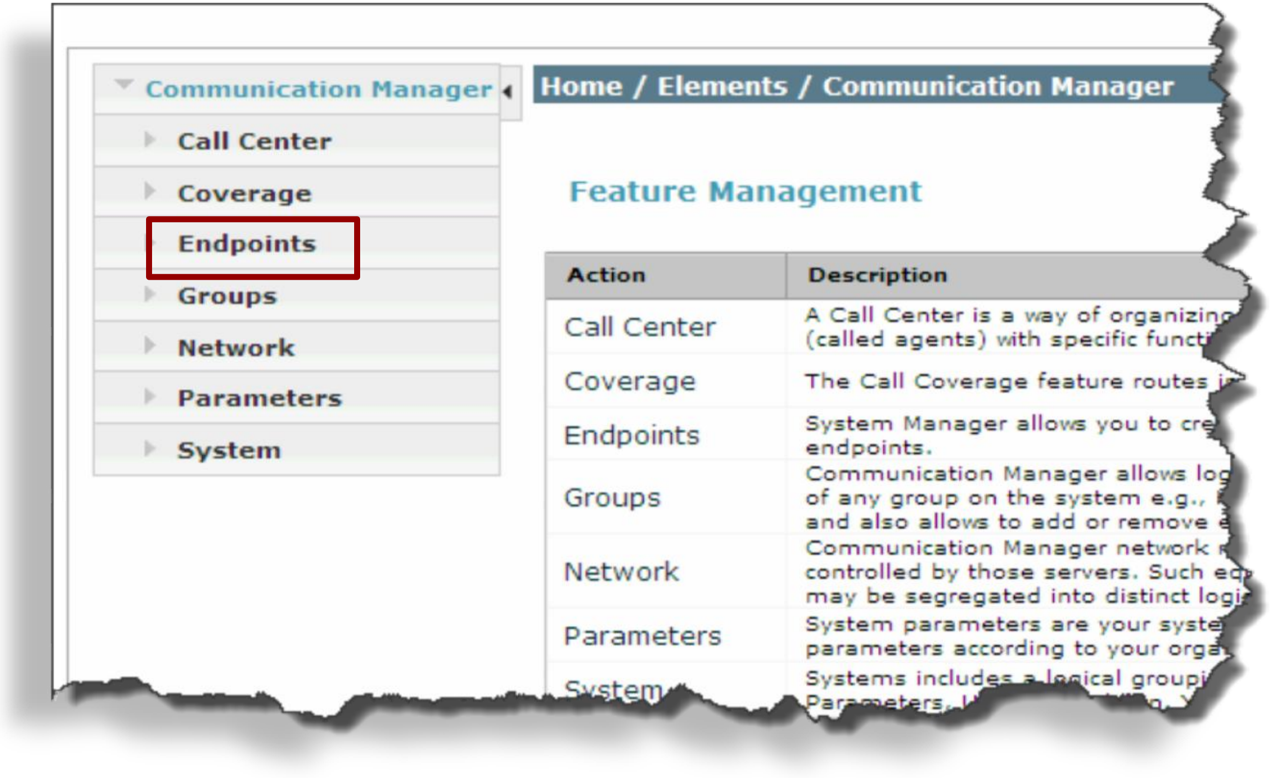
Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway objects

UCM Services

View Communication Manager Data

- Select Endpoints to view the stations configured in CM

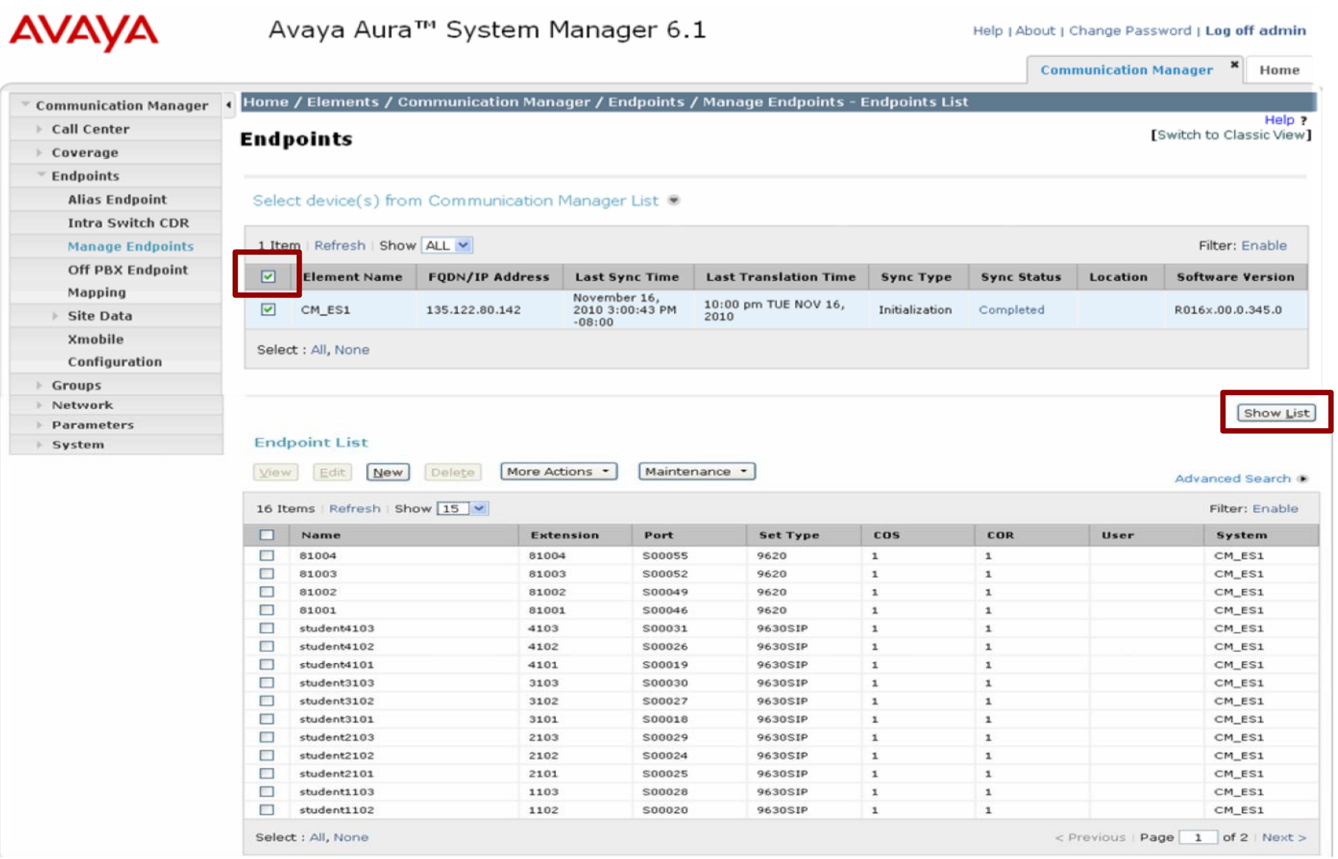


Feature Management

Action	Description
Call Center	A Call Center is a way of organizing (called agents) with specific functi
Coverage	The Call Coverage feature routes i
Endpoints	System Manager allows you to cre endpoints.
Groups	Communication Manager allows log of any group on the system e.g., and also allows to add or remove
Network	Communication Manager network controlled by those servers. Such eq may be segregated into distinct logi
Parameters	System parameters are your syste parameters according to your orga
System	Systems includes a logical groupi Parameters.

View Communication Manager Endpoints

- Select the system and click “show list”.
- That will display the stations define in that CM.
- Shortly, we will create SIP User Communication Profiles and associate them to these CM stations.



Avaya Aura™ System Manager 6.1

Endpoints

Select device(s) from Communication Manager List

1 Item | Refresh | Show ALL   Filter: Enable

☑	Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type	Sync Status	Location	Software Version
☑	CM_ES1	135.122.80.142	November 16, 2010 3:00:43 PM -08:00	10:00 pm TUE NOV 16, 2010	Initialization	Completed		R016x.00.0.345.0

Select : All, None

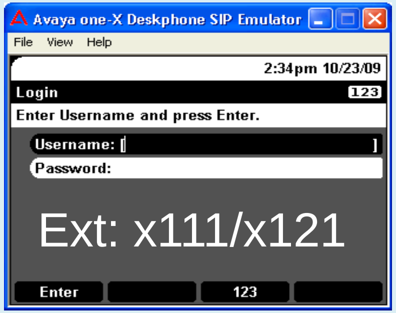
Endpoint List

16 Items | Refresh | Show 15   Filter: Enable

□	Name	Extension	Port	Set Type	COS	COR	User	System
□	81004	81004	S00055	9620	1	1		CM_ES1
□	81003	81003	S00052	9620	1	1		CM_ES1
□	81002	81002	S00049	9620	1	1		CM_ES1
□	81001	81001	S00046	9620	1	1		CM_ES1
□	student4103	4103	S00031	9630SIP	1	1		CM_ES1
□	student4102	4102	S00026	9630SIP	1	1		CM_ES1
□	student4101	4101	S00019	9630SIP	1	1		CM_ES1
□	student3103	3103	S00030	9630SIP	1	1		CM_ES1
□	student3102	3102	S00027	9630SIP	1	1		CM_ES1
□	student3101	3101	S00018	9630SIP	1	1		CM_ES1
□	student2103	2103	S00029	9630SIP	1	1		CM_ES1
□	student2102	2102	S00024	9630SIP	1	1		CM_ES1
□	student2101	2101	S00025	9630SIP	1	1		CM_ES1
□	student1103	1103	S00028	9630SIP	1	1		CM_ES1
□	student1102	1102	S00020	9630SIP	1	1		CM_ES1

Select : All, None   < Previous | Page 1 of 2 | Next >

Advanced SIP Terminals: SIP Users associated with CM Stations



2:34pm 10/23/09

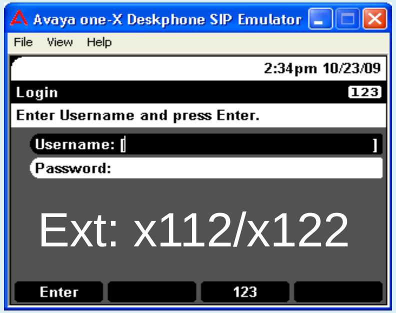
Login 123

Enter Username and press Enter.

Username: [ ]

Password:

Ext: x111/x121



2:34pm 10/23/09

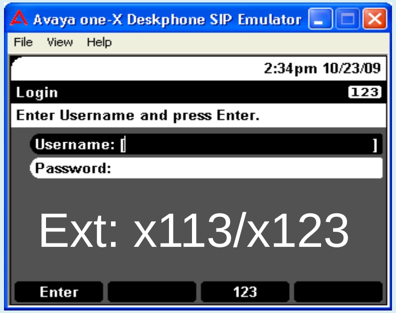
Login 123

Enter Username and press Enter.

Username: [ ]

Password:

Ext: x112/x122



2:34pm 10/23/09

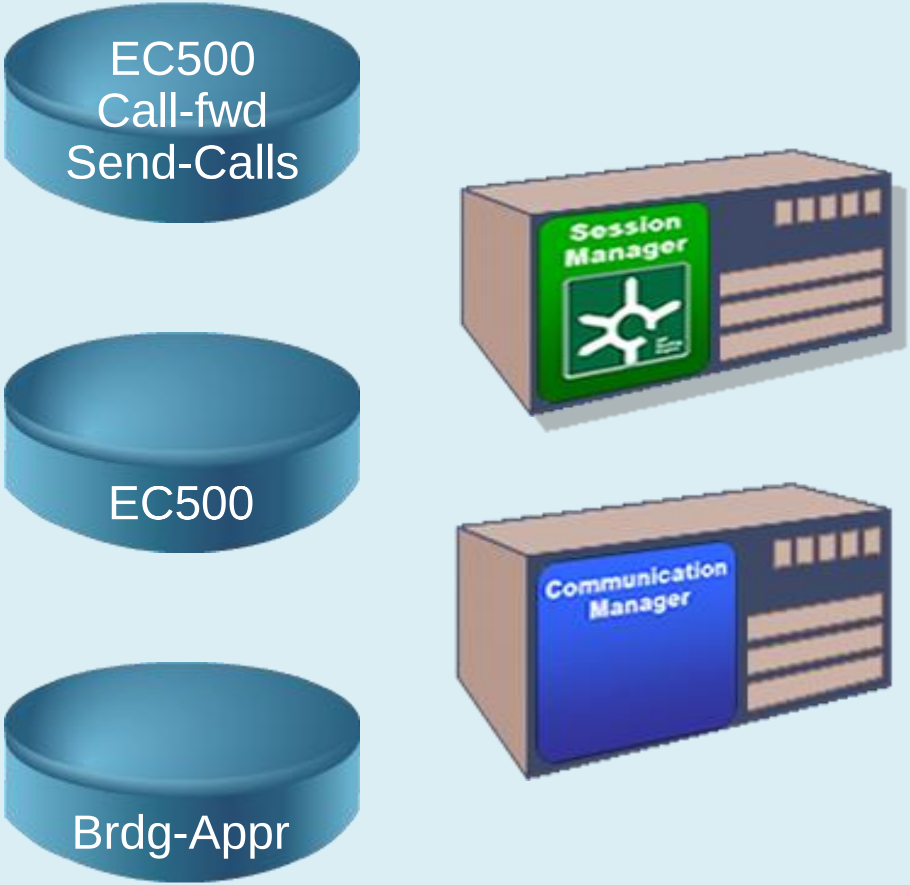
Login 123

Enter Username and press Enter.

Username: [ ]

Password:

Ext: x113/x123



EC500
Call-fwd
Send-Calls

EC500

Brdg-Appr

Exercise: View CM Stations

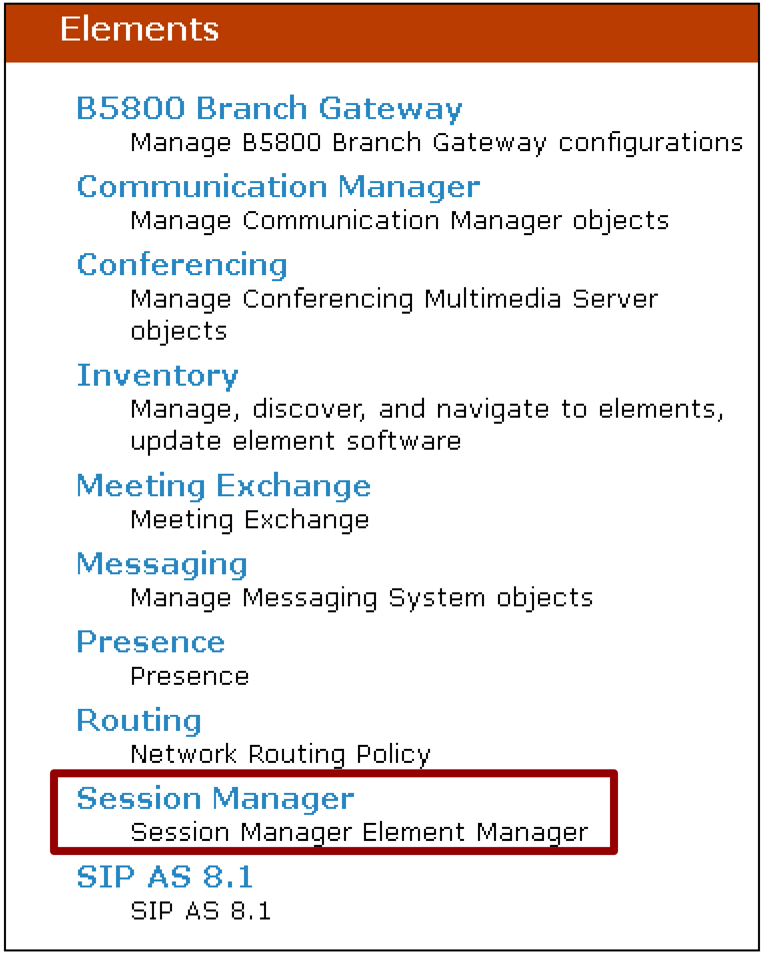
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Once the endpoint list is displayed, select one of your endpoints:
<table>
<tr><th>Student</th><th>Pod 1</th><th>Pod 2</th><th>Pod 3</th><th>Pod 4</th><th>Pod 5</th><th>Pod 6</th></tr>
<tr><td>Student a</td><td>1111
1112
1113</td><td>2111
2112
2113</td><td>3111
3112
3113</td><td>41114
11241
13</td><td>5111
5112
5113</td><td>6111
6112
6113</td></tr>
<tr><td>Student b</td><td>1121
1122
1123</td><td>2121
2122
2123</td><td>3121
3122
3123</td><td>41214
12241
23</td><td>5121
5122
5123</td><td>6121
6122
6123</td></tr>
</table></td></tr>
<tr><td>2</td><td>Review the station details</td></tr>
<tr><td>3</td><td>Take note of Button Assignments.</td></tr>
<tr><td>4</td><td>Close the endpoint without saving changes.</td></tr>
</table>

AVAYA | LEARNING

Configuring Applications and Application Sequences

Defining Applications

Application Configuration will be done in the Session Manager Elements Menu.



Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway configurations

Communication Manager
Manage Communication Manager objects

Conferencing
Manage Conferencing Multimedia Server objects

Inventory
Manage, discover, and navigate to elements, update element software

Meeting Exchange
Meeting Exchange

Messaging
Manage Messaging System objects

Presence
Presence

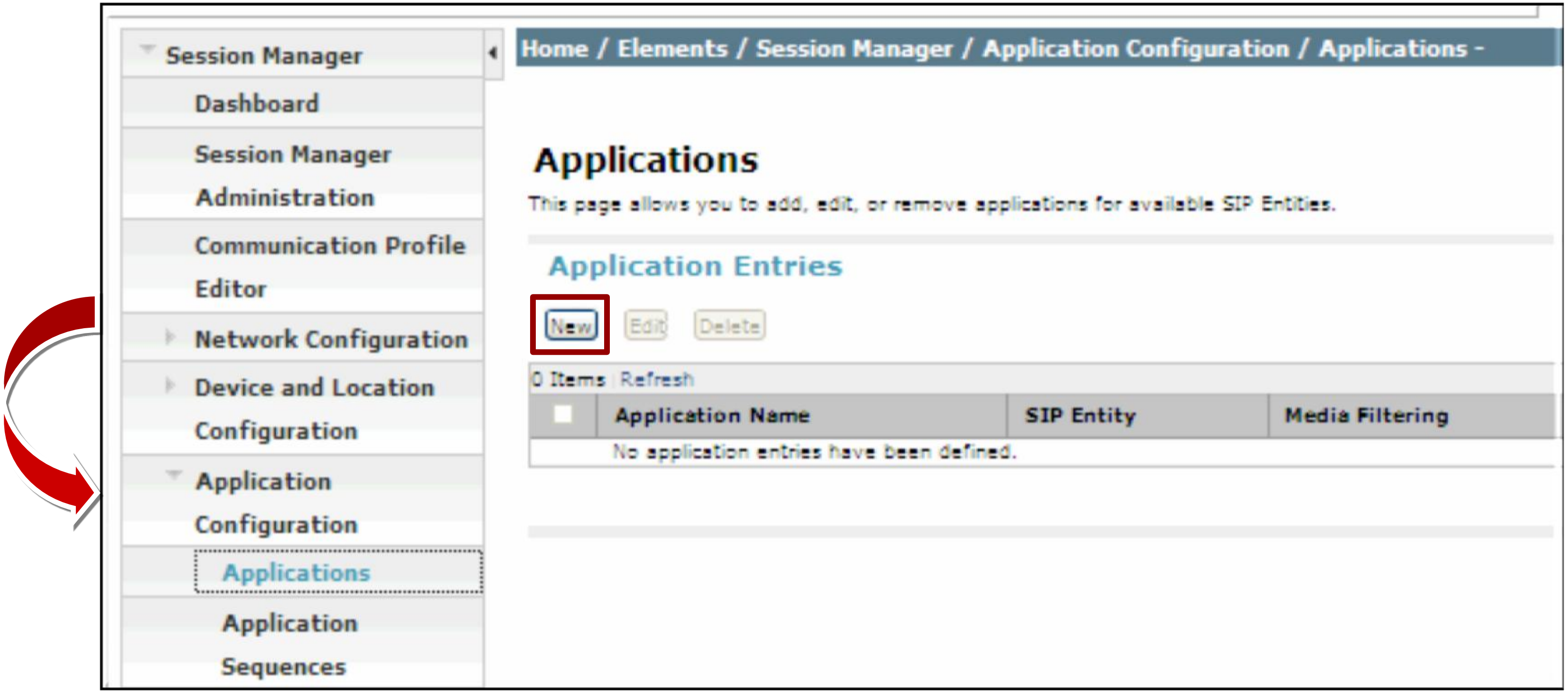
Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Defining Applications (continued)

From the Applications Menu, select New.


Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
Applications
Application Sequences
Home / Elements / Session Manager / Application Configuration / Applications -
New
Edit
Delete
0 Items | Refresh

Applications

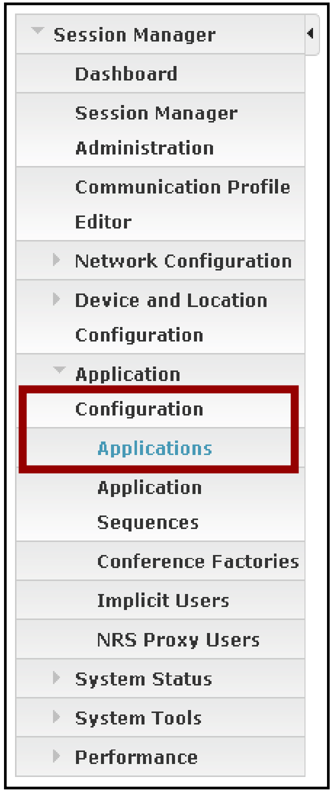
This page allows you to add, edit, or remove applications for available SIP Entities.

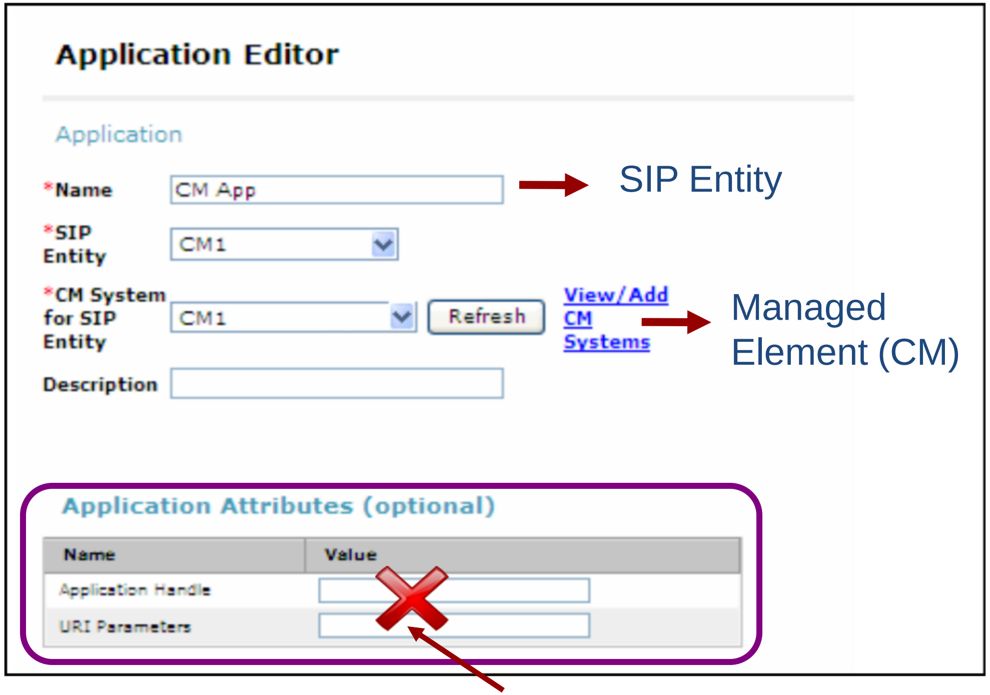
Application Entries

□	Application Name	SIP Entity	Media Filtering
	No application entries have been defined.		

Define the Application for CM

1. Define the name of your CM Application
2. Select your CM SIP Entity
3. Select your CM System for SIP Entity
4. Commit




Application Editor

Application

*Name: CM App

*SIP Entity: CM1

*CM System for SIP Entity: CM1 [Refresh] View/Add CM Systems

Description:

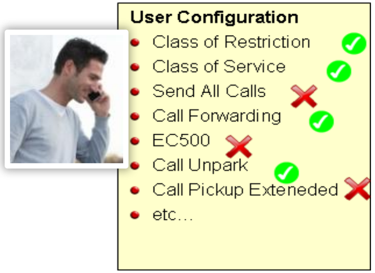
SIP Entity

Managed Element (CM)

Application Attributes (optional)

Name	Value
Application Handle	
URI Parameters	

When creating an Application for CM, you DO NOT enter an application handle. Leave it blank.


User Configuration

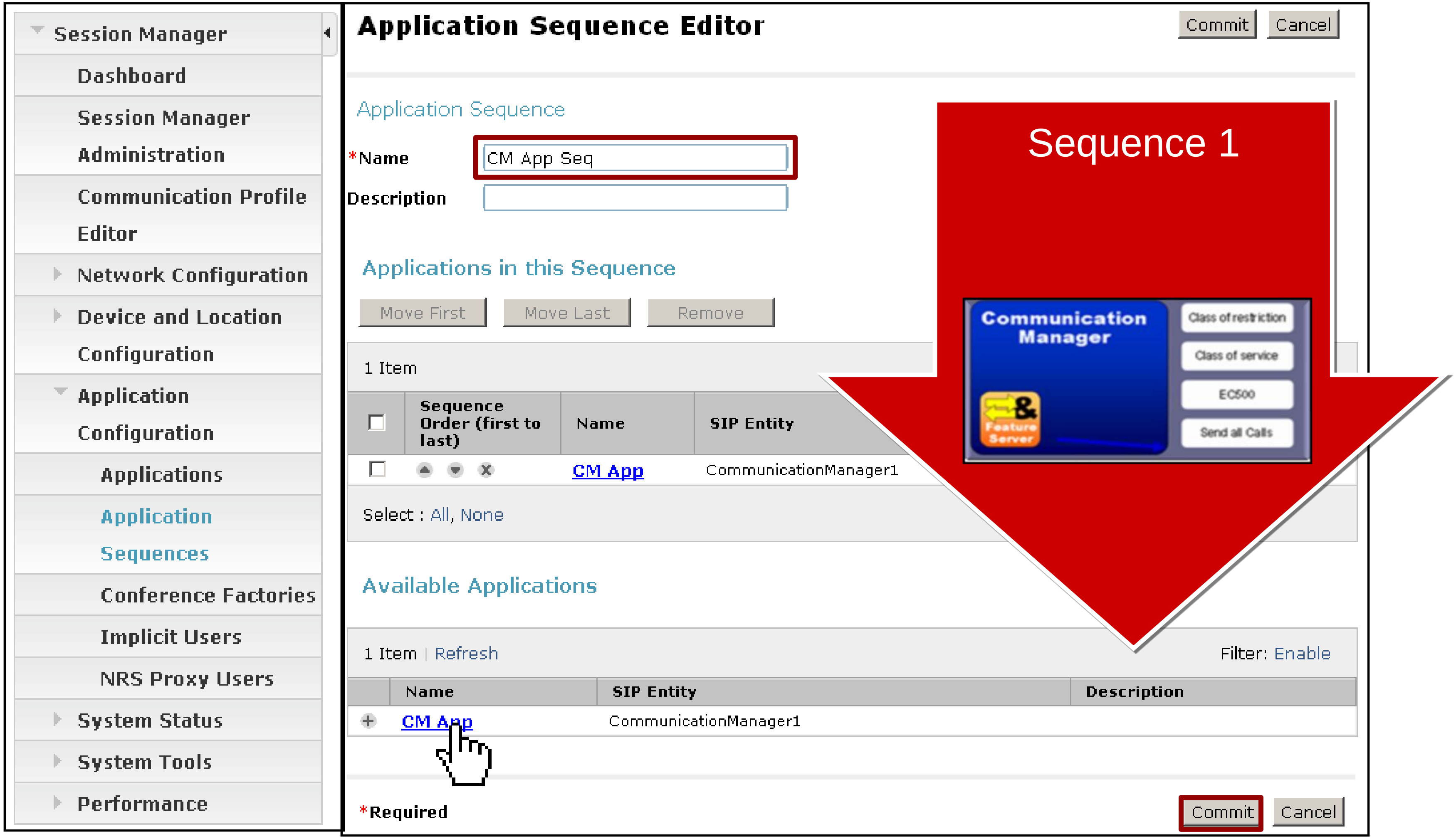
- Class of Restriction ✓
- Class of Service ✓
- Send All Calls ✗
- Call Forwarding ✓
- EC500 ✗
- Call Unpark ✓
- Call Pickup Exteneded ✗
- etc…

Note

CM must first be configured as a SIP entity with entity links.

Define the Application Sequence For CM

- Select the + next to your CM Application to add to Sequence



Application Sequence Editor

Application Sequence

*Name: CM App Seq

Description:

Applications in this Sequence

1 Item

□	Sequence Order (first to last)	Name	SIP Entity
□		CM App	CommunicationManager1

Select : All, None

Available Applications

1 Item | Refresh   Filter: Enable

	Name	SIP Entity	Description
+	CM App	CommunicationManager1	

*Required

Exercise: Create CM Application and Application Sequence

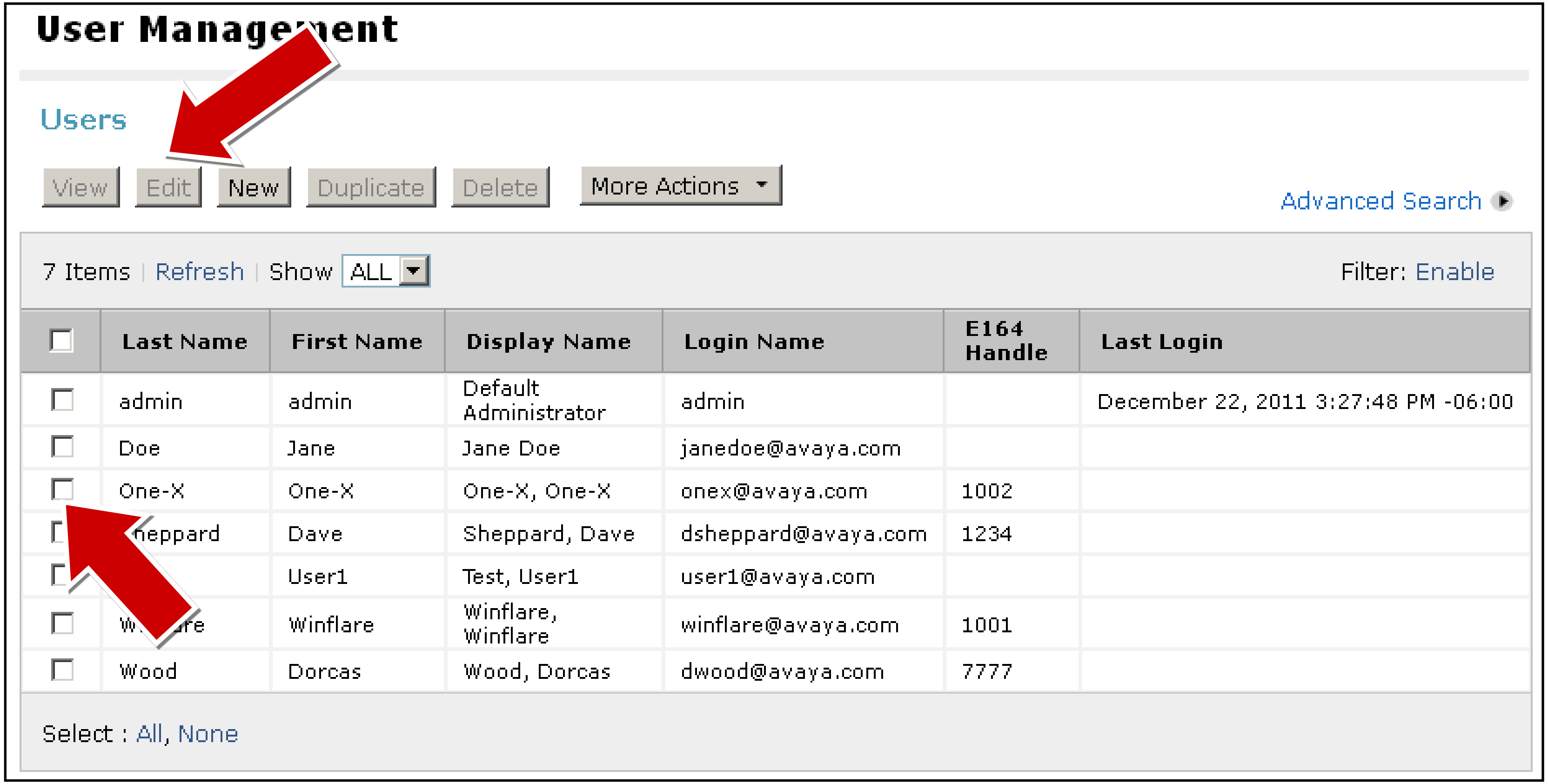
Step	Action
1	**Create a CM Application**
2	Navigate to Session Manager Elements Menu then Select Application
3	Select **New**
4	Application Name: CM1, CM2 add table
5	Select your CM SIP Entity from the SIP Entity drop-down list
6	Select your CM Managed Element from the **CM System for SIP Entity** drop-down list
7	Commit
8	**Create a CM Application Sequence**
9	Navigate to Application Configuration>Application Sequences
10	Select New
11	Application Sequence Name: CM
12	Select the **+** next to your CM Application to add to Sequence
13	Commit

AVAYA | LEARNING

Applying Application Sequences to Users

Applying Application Sequences

- Edit SIP User to apply Application Sequence to User's Communication Profile



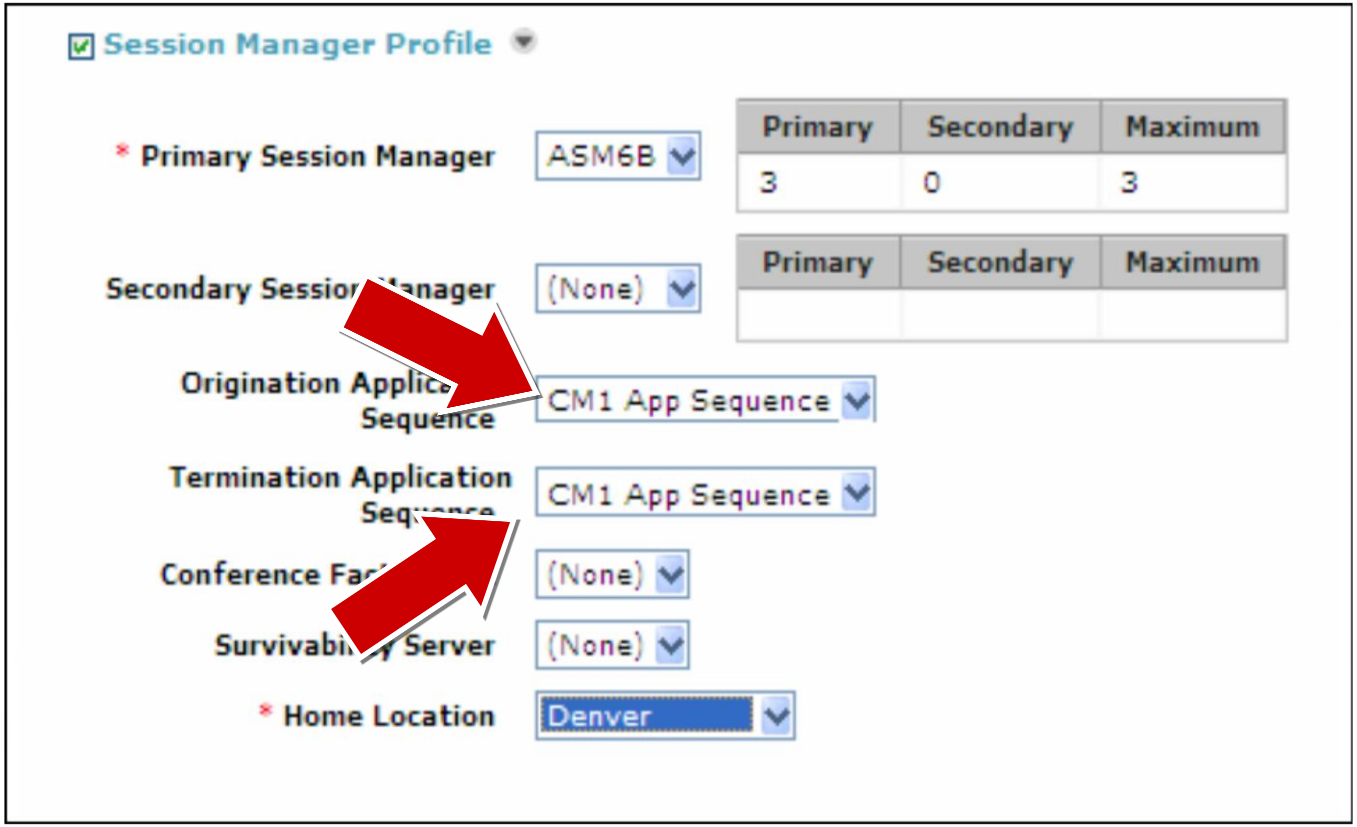
7 Items | Refresh | Show ALL

Filter: Enable

□	Last Name	First Name	Display Name	Login Name	E164 Handle	Last Login
□	admin	admin	Default Administrator	admin		December 22, 2011 3:27:48 PM -06:00
□	Doe	Jane	Jane Doe	janedoe@avaya.com		
□	One-X	One-X	One-X, One-X	onex@avaya.com	1002	
□	heppard	Dave	Sheppard, Dave	dsheppard@avaya.com	1234	
□		User1	Test, User1	user1@avaya.com		
□	W re	Winflare	Winflare, Winflare	winflare@avaya.com	1001	
□	Wood	Dorcas	Wood, Dorcas	dwood@avaya.com	7777	

Select : All, None

Applying Application Sequences (continued)



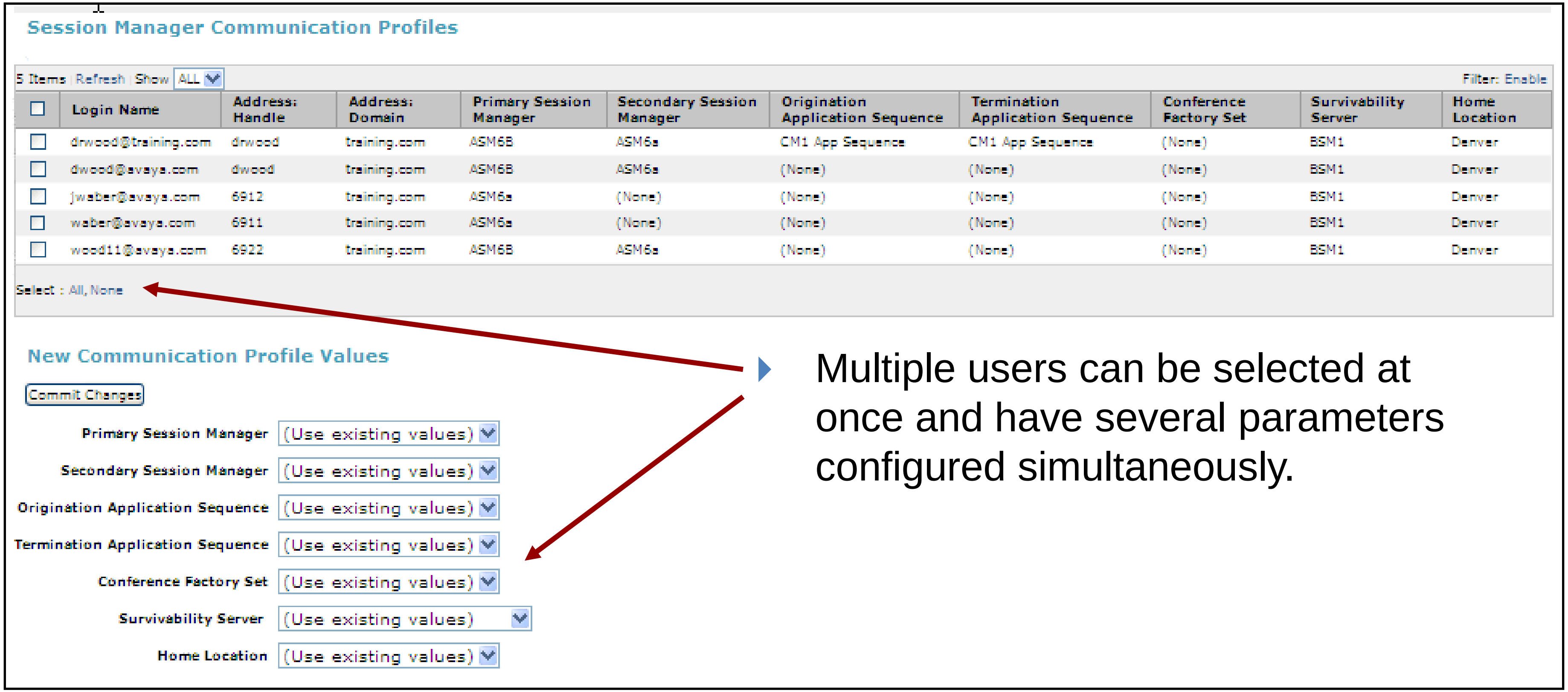
☑ Session Manager Profile

		Primary	Secondary	Maximum
* Primary Session Manager	ASM6B	3	0	3
Secondary Session Manager	(None)			

Origination Application Sequence	CM1 App Sequence
Termination Application Sequence	CM1 App Sequence
Conference Factory Set	(None)
Survivability Server	(None)
* Home Location	Denver

Applying Application Sequences in Bulk

Navigate to Session Manager Elements Menu>>Communication Profile Editor



Session Manager Communication Profiles

5 Items | Refresh | Show ALL

Filter: Enable

☐	Login Name	Address: Handle	Address: Domain	Primary Session Manager	Secondary Session Manager	Origination Application Sequence	Termination Application Sequence	Conference Factory Set	Survivability Server	Home Location
☐	drwood@training.com	drwood	training.com	ASM6B	ASM6a	CM1 App Sequence	CM1 App Sequence	(None)	BSM1	Denver
☐	dwood@avaya.com	dwood	training.com	ASM6B	ASM6a	(None)	(None)	(None)	BSM1	Denver
☐	jweber@avaya.com	6912	training.com	ASM6a	(None)	(None)	(None)	(None)	BSM1	Denver
☐	weber@avaya.com	6911	training.com	ASM6a	(None)	(None)	(None)	(None)	BSM1	Denver
☐	wood11@avaya.com	6922	training.com	ASM6B	ASM6a	(None)	(None)	(None)	BSM1	Denver

Select : All, None

New Communication Profile Values

Commit Changes

Primary Session Manager	(Use existing values)
Secondary Session Manager	(Use existing values)
Origination Application Sequence	(Use existing values)
Termination Application Sequence	(Use existing values)
Conference Factory Set	(Use existing values)
Survivability Server	(Use existing values)
Home Location	(Use existing values)

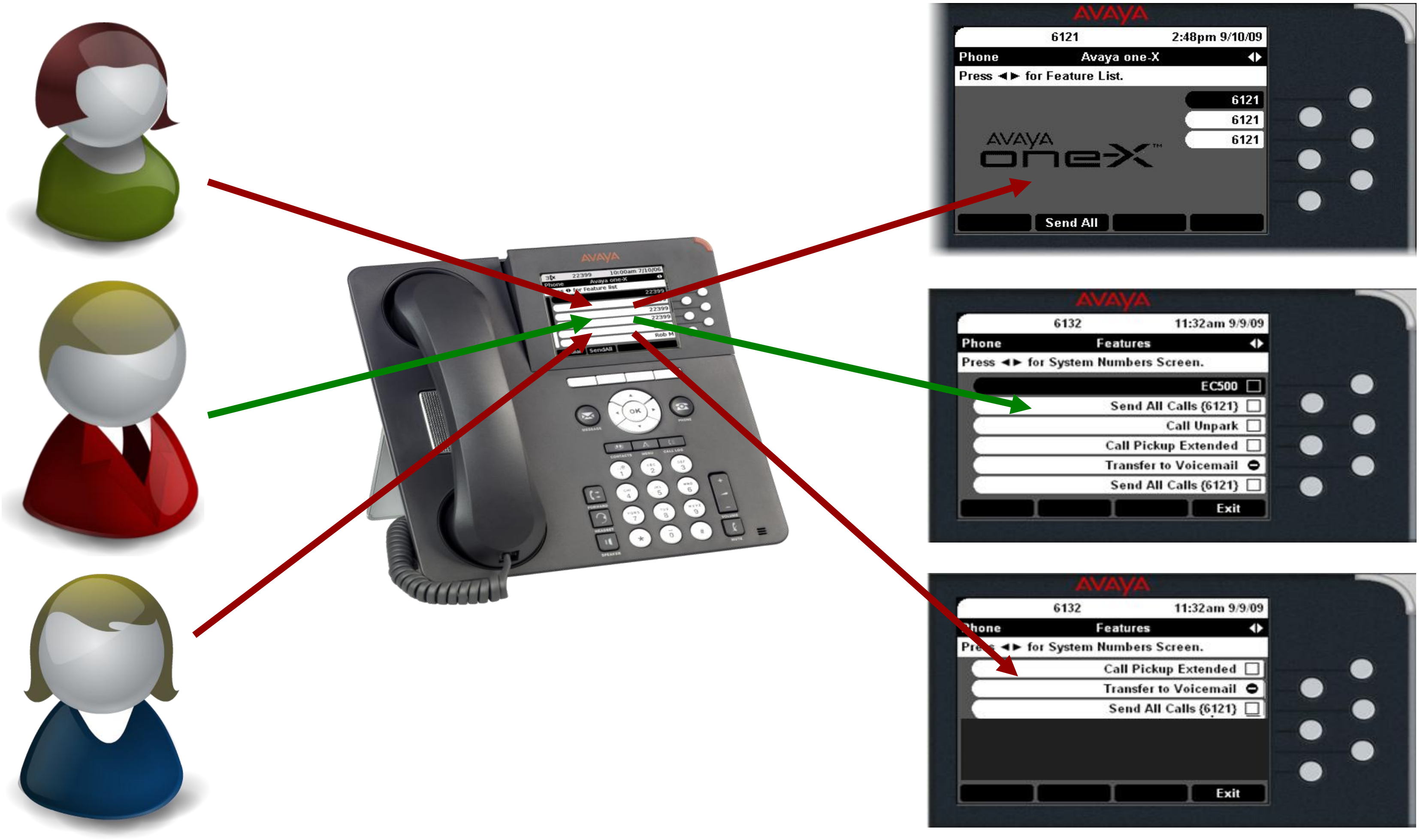
- Multiple users can be selected at once and have several parameters configured simultaneously.

PPM

Personal Profile Manager (PPM)

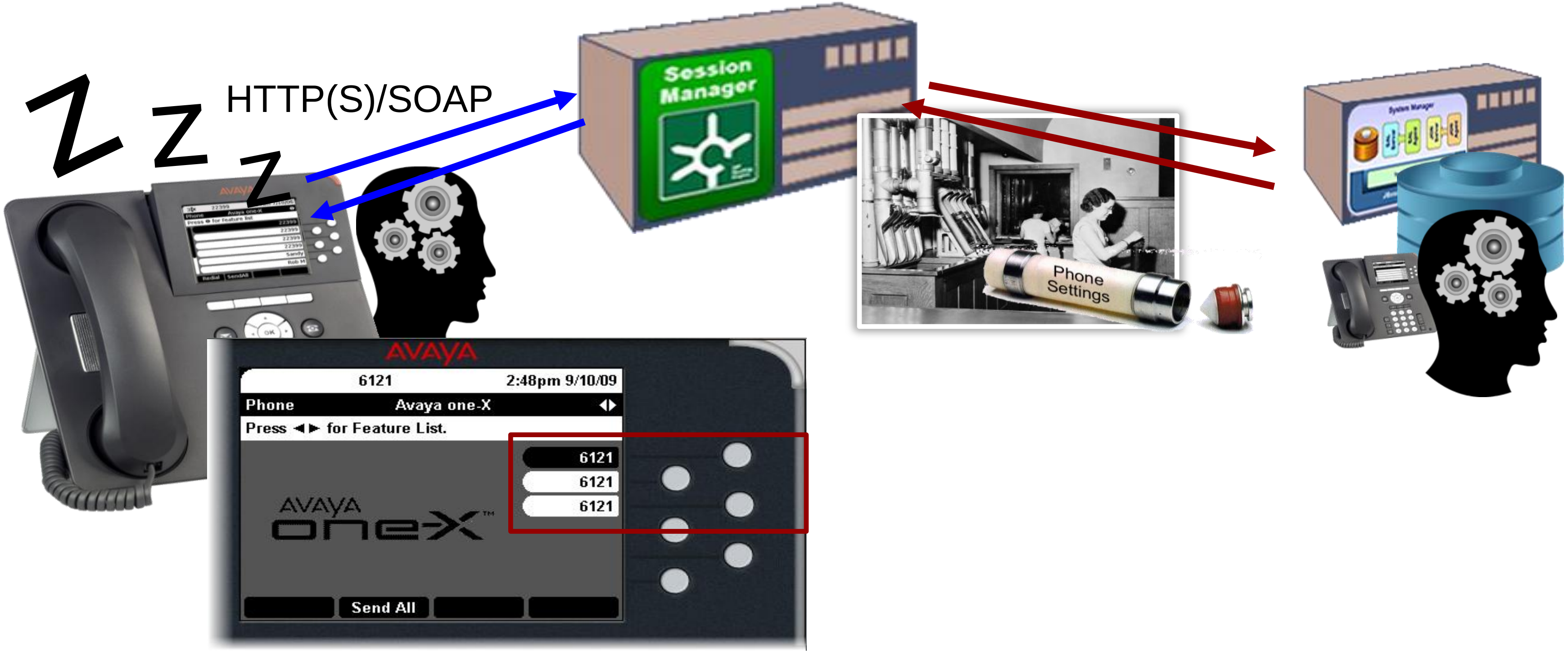
Personal Profile Manager – PPM

- Before Different users… Different settings

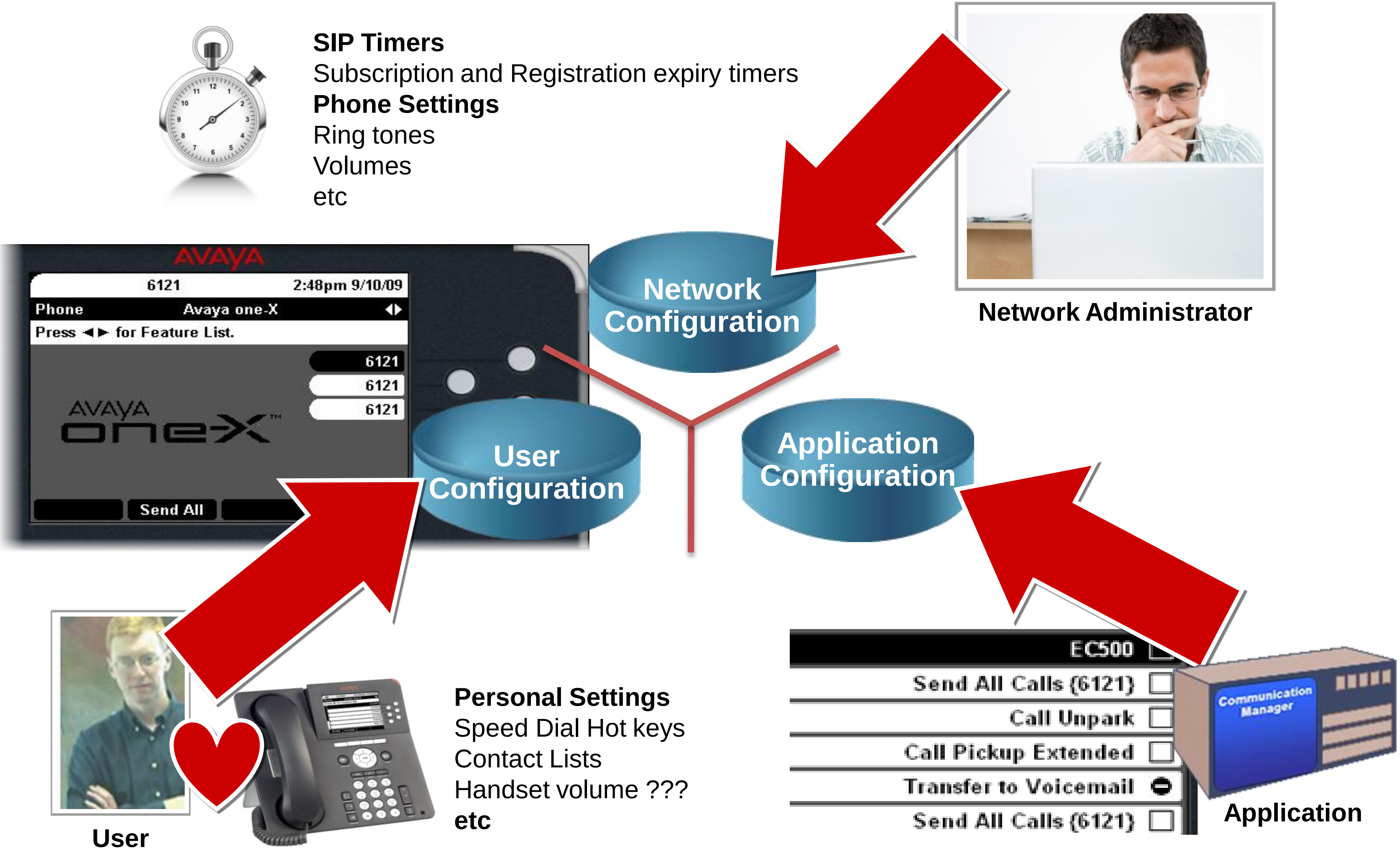


Personal Profile Manager

- PPM is downloaded over http(s) using SOAP messages, not SIP.



PPM Three Types of Data



SIP Timers
Subscription and Registration expiry timers
Phone Settings
Ring tones
Volumes
etc

Personal Settings
Speed Dial Hot keys
Contact Lists
Handset volume ???
etc

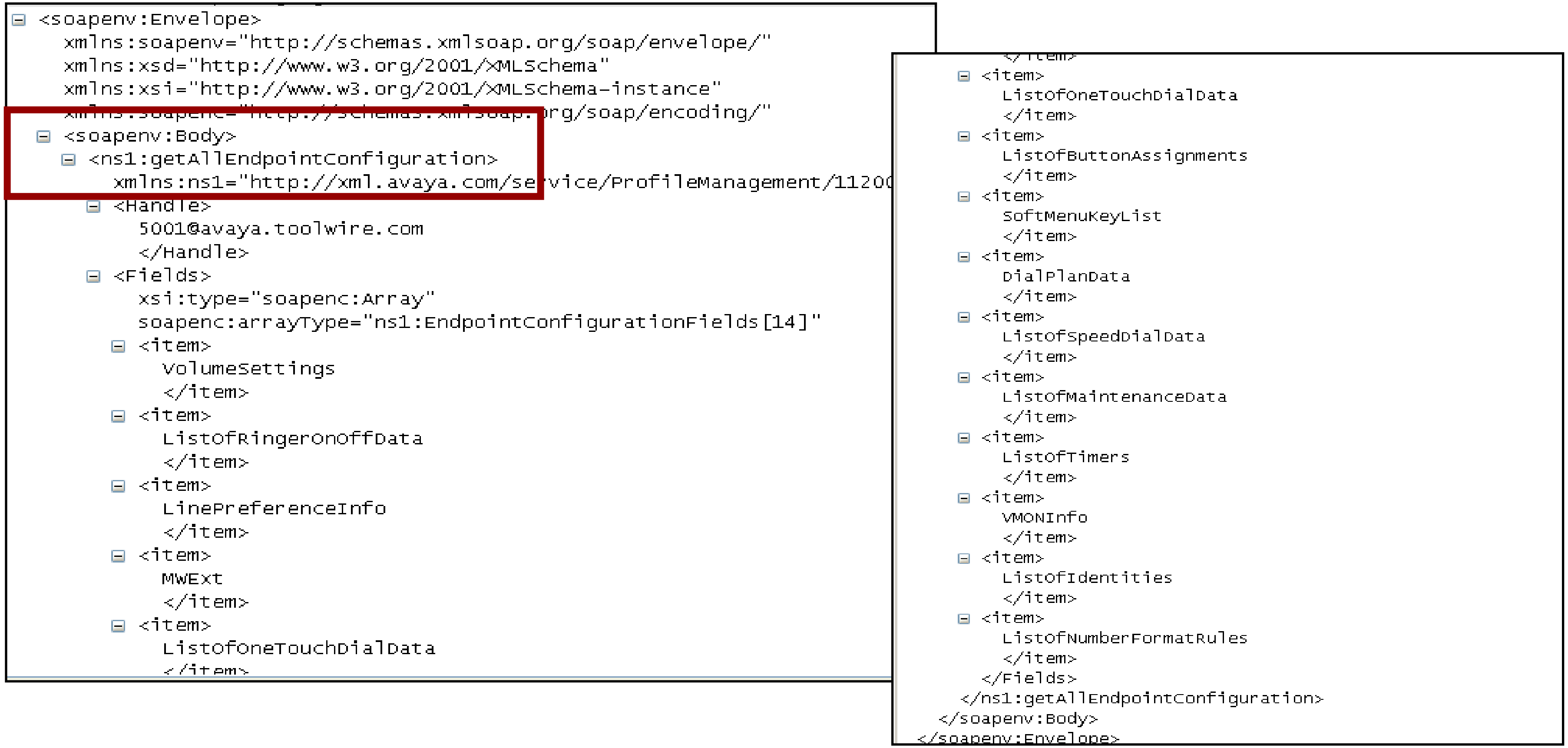
PPM Requests

SM 6.1 Supported PPM Requests and Clients for Session Manager

Method	SM	Dev – Connect	Notes
addContact	5.2	SM 5.2	
deleteContact	5.2	SM 5.2	
getAllEndpointConfiguration	5.2	SM 5.2	
getContactList	5.2	SM 5.2	
getDeviceData	5.2	SM 6.0	In 5.2, this contains default data in the response.
getHomeCapabilities	5.2	SM 5.2	
getHomeServer	5.2	SM 5.2	
getPermissionType	n/a	n/a	Default data in the response.
setDeviceData	5.2	SM 6.0	In 5.2, this contains default data in the response.
setVolumeSettings	5.2	SM 6.0	A separate getVolumeSettings method is not needed as it is included in the getAllEndpointConfiguration response.
updateContact	6.0	SM 6.0	
searchContact	6.1	SM 6.1	Supported for backwards compatibility with SIP 2.6 phones. Use searchUser for new applications. *Note: method details to be added to this document.*
searchContactCount	6.1	SM 6.1	Supported for backwards compatibility with SIP 2.6 phones. *Note: method details to be added to this document!*
searchUser	6.1	SM 6.1	Replace searchContact
searchUserCount	6.1	SM 6.1	Not currently supported because no applications are planning t o use it.

Example: getAllEndpointConfiguration Request

- This is an example of the content of the HTTP Request message to getAllEndpointConfiguration from a SIP endpoint to Session Manager’s PPM service.

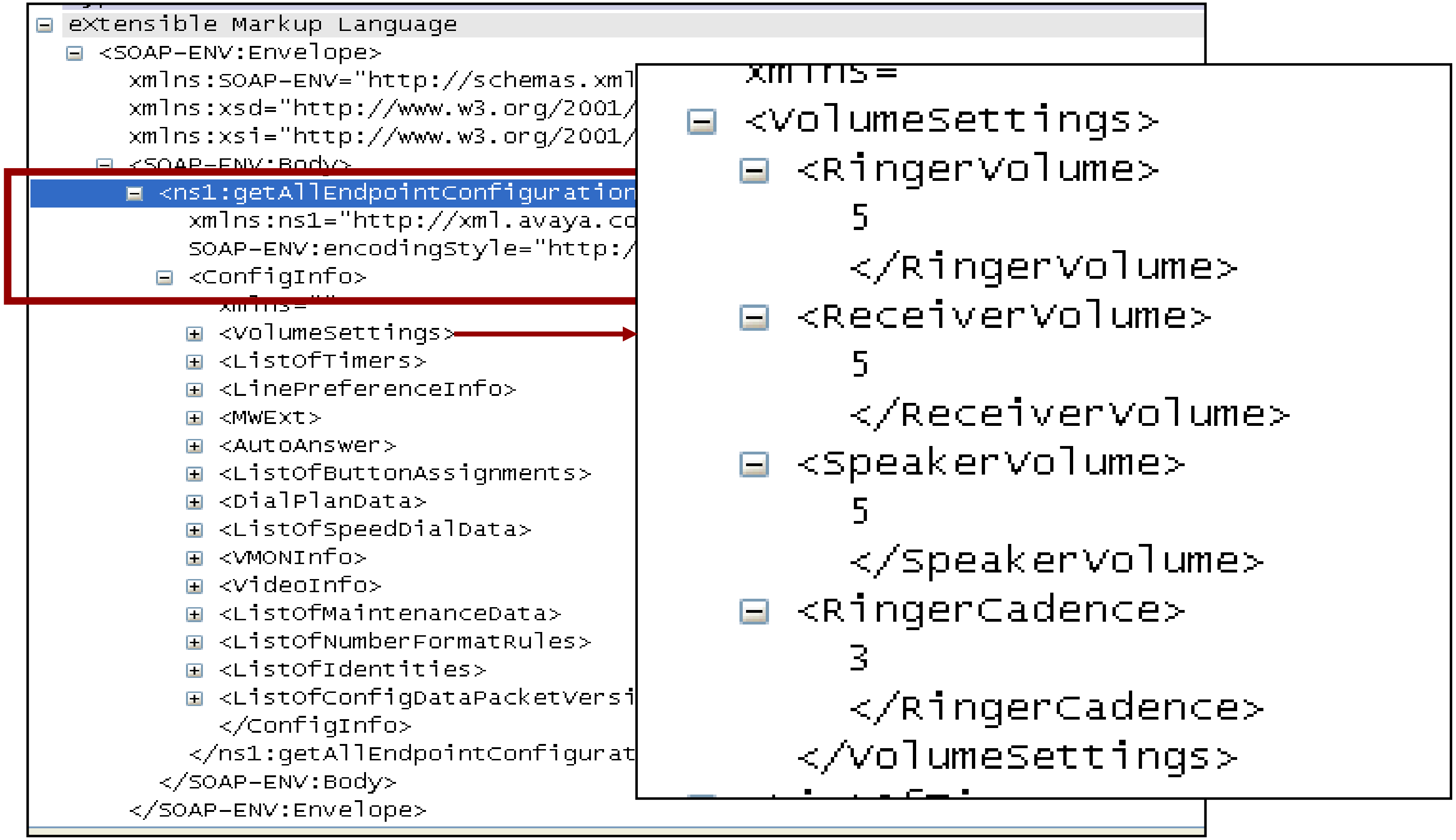


```
<soapenv:Envelope>
   xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
   <soapenv:Body>
      <ns1:getAllEndpointConfiguration>
         xmlns:ns1="http://xml.avaya.com/service/ProfileManagement/11200
         <Handle>
            5001@avaya.toolwire.com
            </Handle>
         <Fields>
            xsi:type="soapenc:Array"
            soapenc:arrayType="ns1:EndpointConfigurationFields[14]"
            <item>
               VolumeSettings
               </item>
            <item>
               ListofRingerOnOffData
               </item>
            <item>
               LinePreferenceInfo
               </item>
            <item>
               MWExt
               </item>
            <item>
               ListofOneTouchDialData
               </item>
```

```
               </item>
            <item>
               ListofOneTouchDialData
               </item>
            <item>
               ListofButtonAssignments
               </item>
            <item>
               SoftMenuKeyList
               </item>
            <item>
               DialPlanData
               </item>
            <item>
               ListofSpeedDialData
               </item>
            <item>
               ListofMaintenanceData
               </item>
            <item>
               ListofTimers
               </item>
            <item>
               VMONInfo
               </item>
            <item>
               ListofIdentities
               </item>
            <item>
               ListofNumberFormatRules
               </item>
            </Fields>
         </ns1:getAllEndpointConfiguration>
      </soapenv:Body>
   </soapenv:Envelope>
```

Example: getAllEndpointConfiguration Response

- This is an example of the content of the HTTP Response message to the phone. For example, the volume settings.

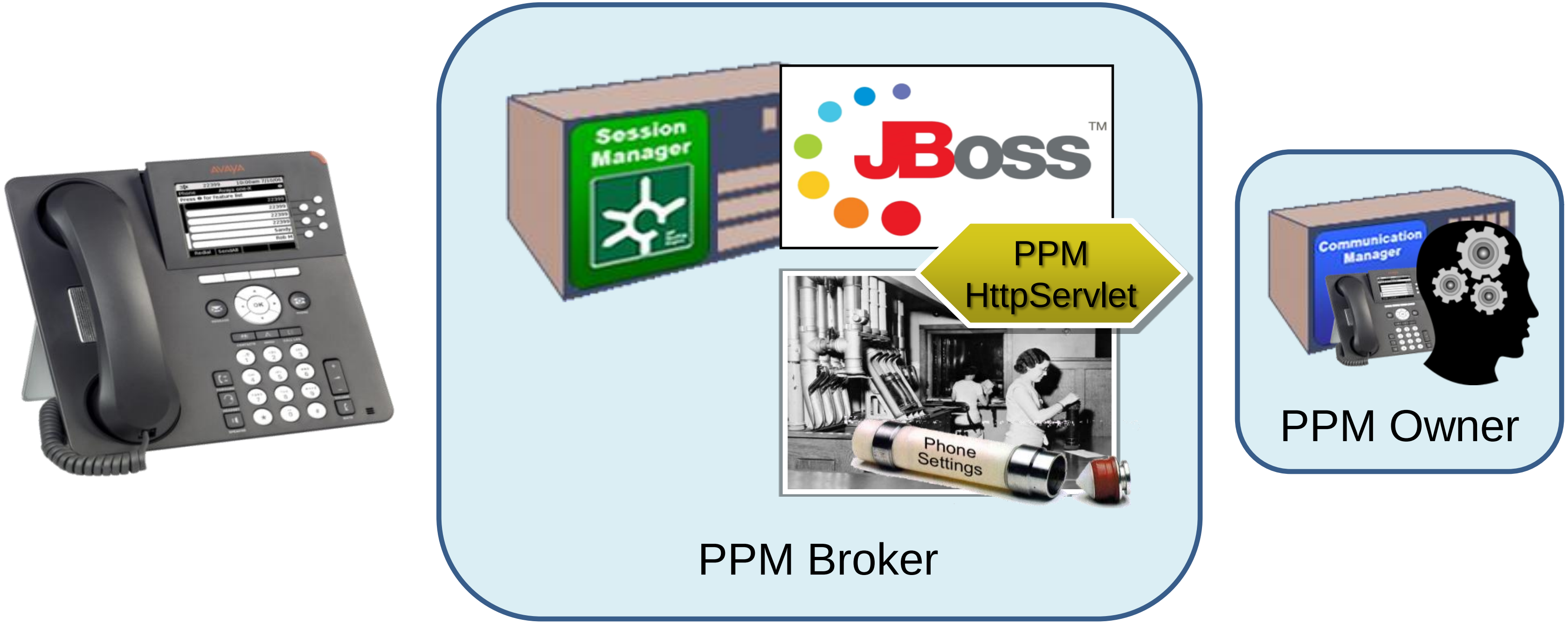


```
⊟ extensible Markup Language
  ⊟ <SOAP-ENV:Envelope>
      xmlns:SOAP-ENV="http://schemas.xml
      xmlns:xsd="http://www.w3.org/2001/
      xmlns:xsi="http://www.w3.org/2001/
    ⊟ <SOAP-ENV:Body>
      ⊟ <ns1:getAllEndpointConfiguration
          xmlns:ns1="http://xml.avaya.co
          SOAP-ENV:encodingStyle="http:/
        ⊟ <ConfigInfo>
            xmlns=""
          ⊞ <VolumeSettings>
          ⊞ <ListofTimers>
          ⊞ <LinePreferenceInfo>
          ⊞ <MWExt>
          ⊞ <AutoAnswer>
          ⊞ <ListofButtonAssignments>
          ⊞ <DialPlanData>
          ⊞ <ListofSpeedDialData>
          ⊞ <VMONInfo>
          ⊞ <VideoInfo>
          ⊞ <ListofMaintenanceData>
          ⊞ <ListofNumberFormatRules>
          ⊞ <ListofIdentities>
          ⊞ <ListofConfigDataPacketVersi
            </ConfigInfo>
          </ns1:getAllEndpointConfigurat
        </SOAP-ENV:Body>
      </SOAP-ENV:Envelope>
```

```
   xmlns=
⊟ <VolumeSettings>
  ⊟ <RingerVolume>
      5
      </RingerVolume>
  ⊟ <ReceiverVolume>
      5
      </ReceiverVolume>
  ⊟ <SpeakerVolume>
      5
      </SpeakerVolume>
  ⊟ <RingerCadence>
      3
      </RingerCadence>
    </VolumeSettings>
```

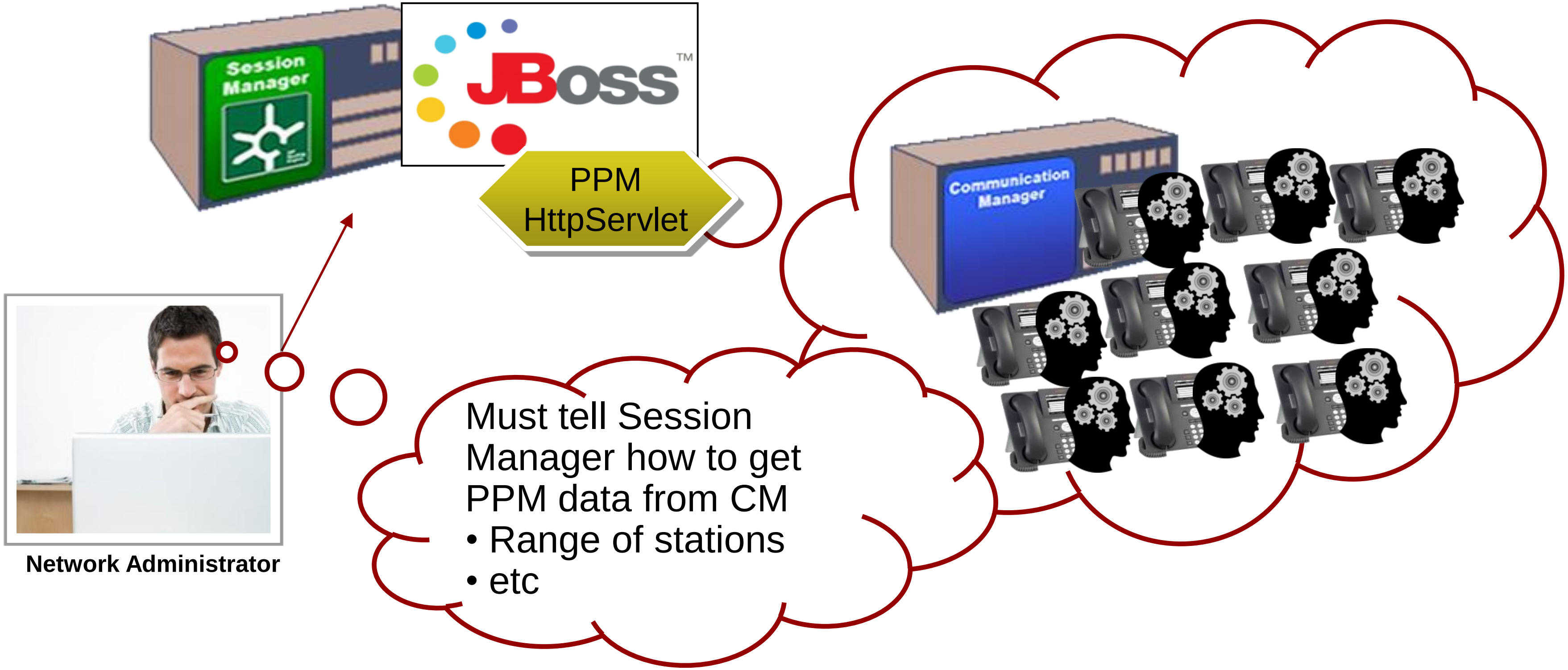
Ownership of Station

- When you associated a SIP User to a CM station then CM controls its telephony features.



Configuration

- If the station is owned by another “entity” we need to somehow share the information with System Manager about that station. This is NOT a SIP relationship.
- In the next slides, we’ll look at how to associate SIP endpoints with CM stations.



PPM HttpServlet

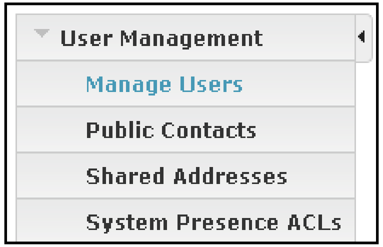
Must tell Session Manager how to get PPM data from CM
• Range of stations
• etc

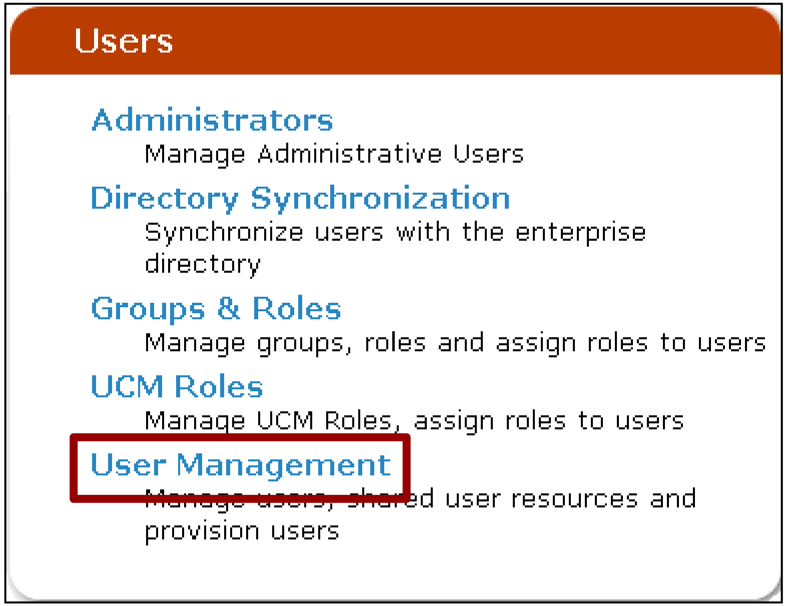
Network Administrator

Associating Communication Manager Stations to SIP Endpoints

Review – Creating a SIP User Communication Profile

1. Add first/last name
2. Login name: you@avaya.com (email address format)
3. Password: must be min. 7 digits alpha-numeric
4. Commit




Users

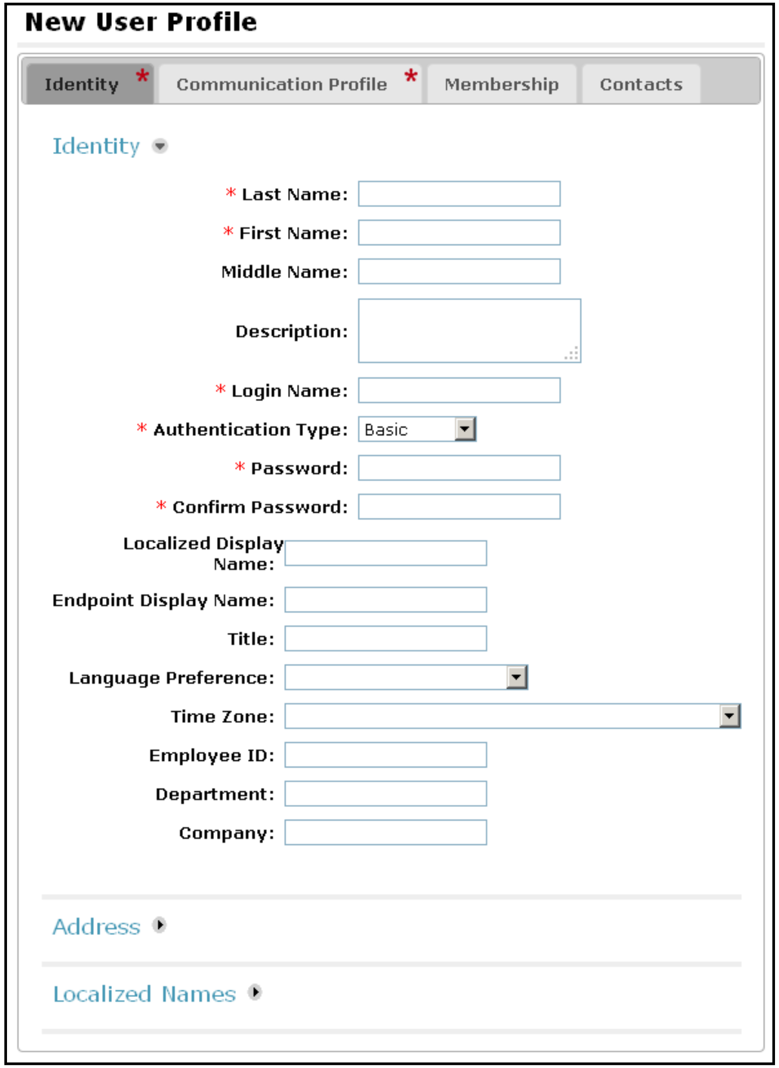
Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

Groups & Roles
Manage groups, roles and assign roles to users

UCM Roles
Manage UCM Roles, assign roles to users

User Management
Manage users, shared user resources and provision users


New User Profile

Identity * | Communication Profile * | Membership | Contacts

Identity

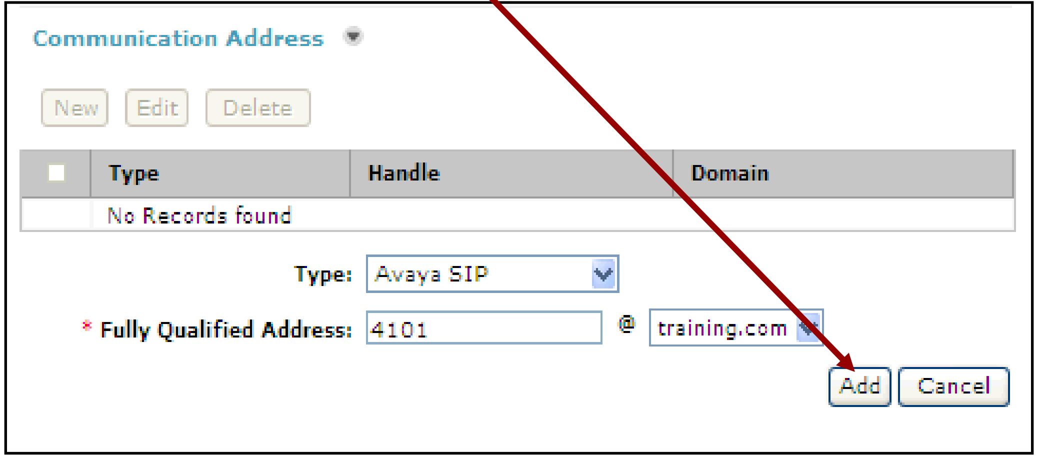
* Last Name:
* First Name:
Middle Name:
Description:
* Login Name:
* Authentication Type: Basic
* Password:
* Confirm Password:
Localized Display Name:
Endpoint Display Name:
Title:
Language Preference:
Time Zone:
Employee ID:
Department:
Company:

Address

Localized Names

Review – Communication Profile

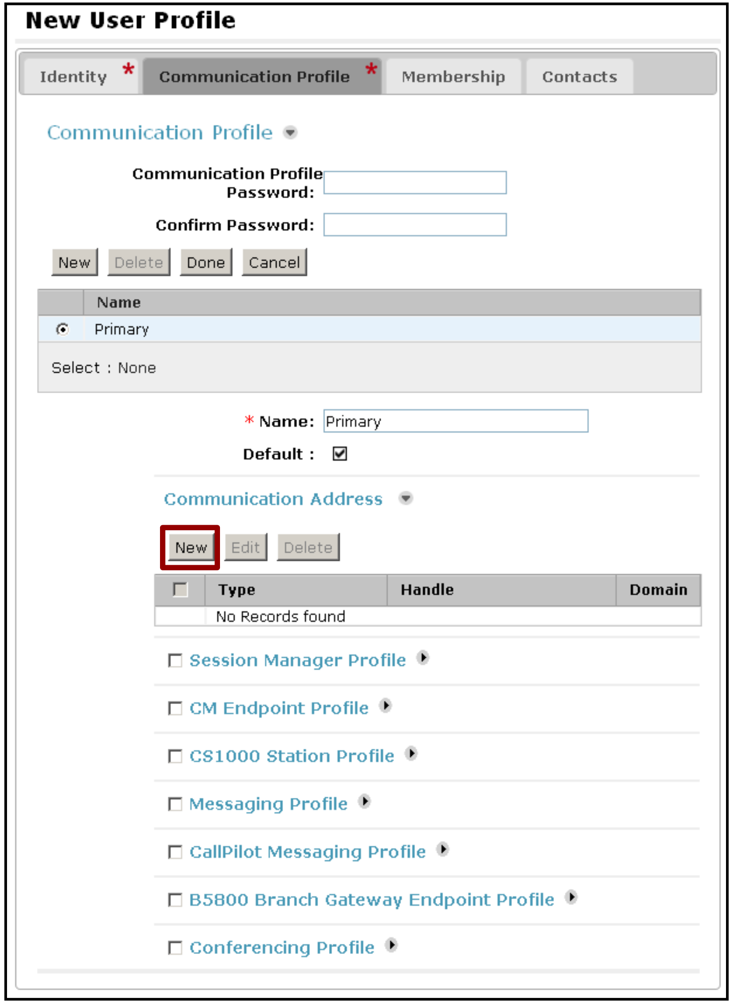
1. Enter Password: 123456
2. Select **New** Communication Address
3. Type: Avaya SIP
4. Fully Qualified Address: x1X1@training.com
5. Select **Add**


Communication Address

☐	Type	Handle	Domain
	No Records found		

Type: Avaya SIP

* Fully Qualified Address: 4101 @ training.com


New User Profile

Communication Profile

Communication Profile Password:

Confirm Password:

	Name
●	Primary

Select : None

* Name: Primary

Default : ☑

Communication Address

☐	Type	Handle	Domain
	No Records found		

☐ Session Manager Profile

☐ CM Endpoint Profile

☐ CS1000 Station Profile

☐ Messaging Profile

☐ CallPilot Messaging Profile

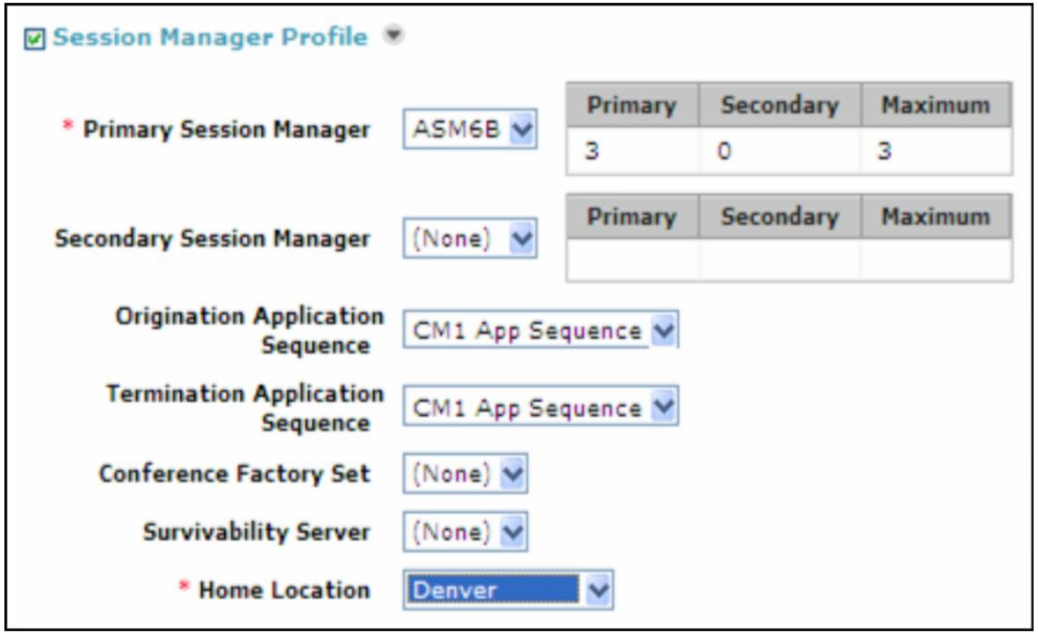
☐ B5800 Branch Gateway Endpoint Profile

☐ Conferencing Profile

New – Communication Profile

1. Select Primary Session Manager
2. **Select CMx for both Origination and Termination Application Sequences**
3. Select a Home Location

This parameter is what tells Session Manager that a SIP endpoint has features and must be routed accordingly for feature application.



☑ Session Manager Profile

* Primary Session Manager: ASM6B

Primary	Secondary	Maximum
3	0	3

Secondary Session Manager: (None)

Primary	Secondary	Maximum

Origination Application Sequence: CM1 App Sequence

Termination Application Sequence: CM1 App Sequence

Conference Factory Set: (None)

Survivability Server: (None)

* Home Location: Denver

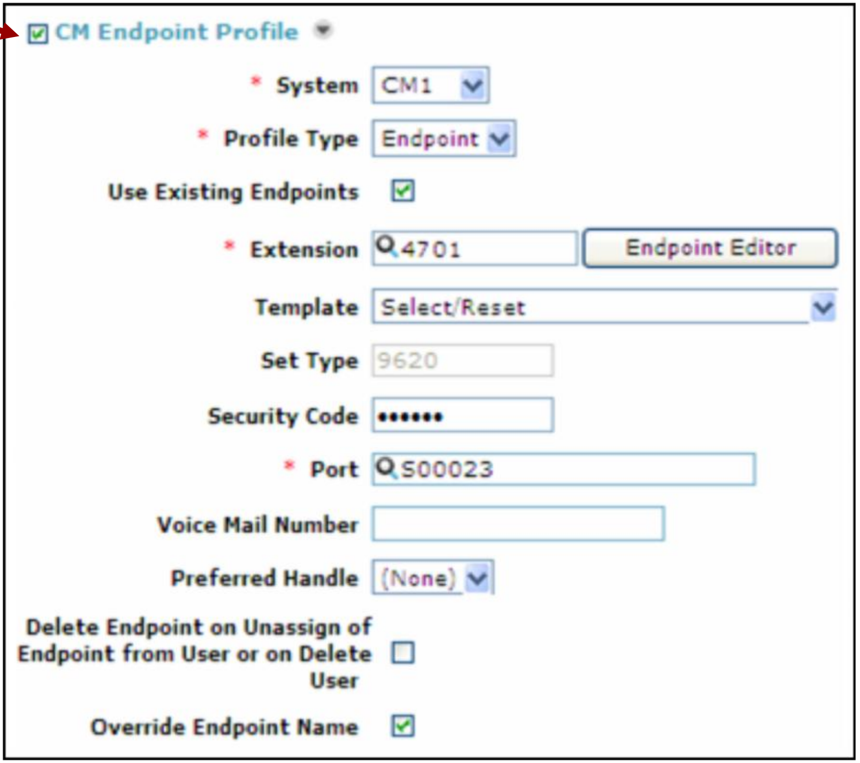
Assigning a CM station to SIP Communication Profiles

1. Check box for CM Endpoint Profile.
2. Select System: CMx
3. Profile Type: Endpoint
4. Check ‘Use Existing Endpoints’
5. Select your x101 station

Enter a Security Code = 123456

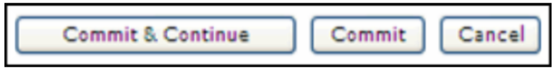
Let everything else be default

Commit



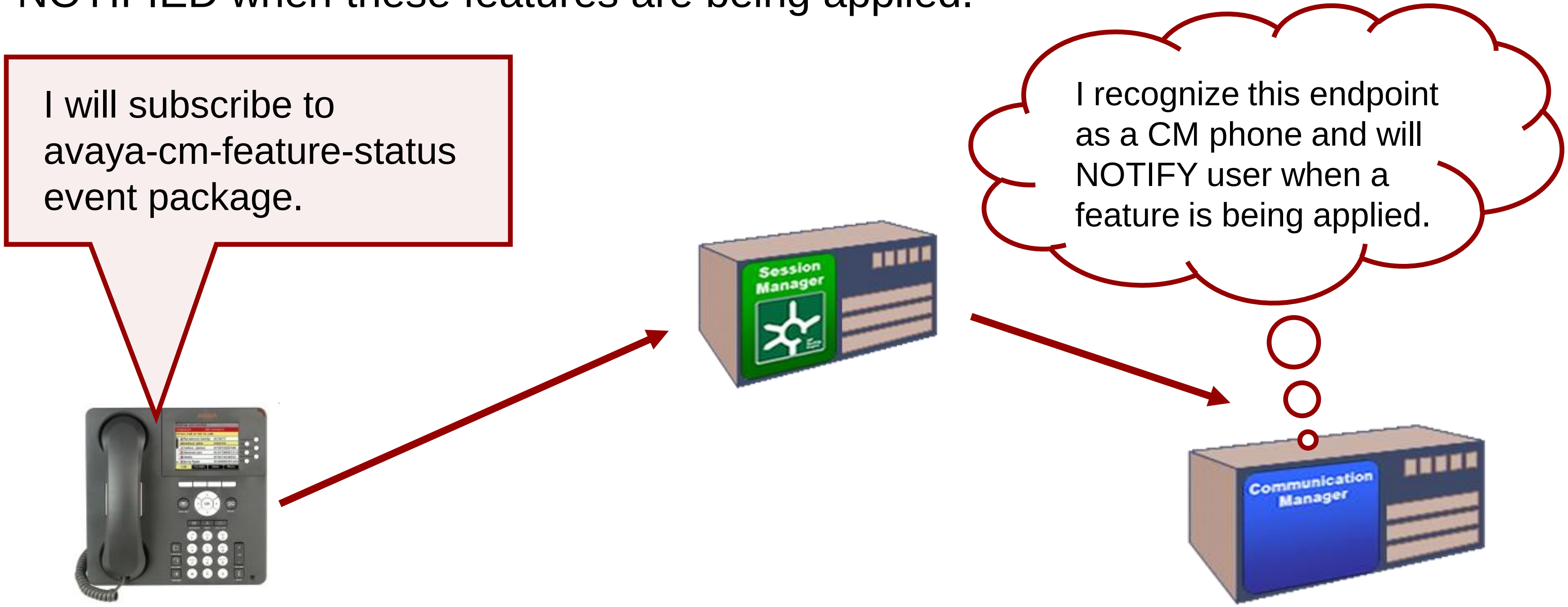
☑ CM Endpoint Profile

* System	CM1
* Profile Type	Endpoint
Use Existing Endpoints	☑
* Extension	4701
Template	Select/Reset
Set Type	9620
Security Code	••••••
* Port	S00023
Voice Mail Number	
Preferred Handle	(None)
Delete Endpoint on Unassign of Endpoint from User or on Delete User	□
Override Endpoint Name	☑



SUBSCRIBE and NOTIFY Messages

- The IETF defines the number of features for a native SIP phone at around 30.
- Advanced SIP phones, those associated to CM stations, support approximately all of Avaya 700 telephony features.
- How do these phones get access to CM telephony features? By subscribing to certain Avaya features using the SUBSCRIBE message and then in turn being NOTIFIED when these features are being applied.



I will subscribe to avaya-cm-feature-status event package.

I recognize this endpoint as a CM phone and will NOTIFY user when a feature is being applied.

Events & Notifications

- Once the phone registers, you will see these SUBSCRIBE and NOTIFY messages in the trace.
- There are a total 5 event packages.

Dialog

message-summary

Avaya-cm feature-status

Avaya-css-profile

Registration-event-package

SIP Endpoint vs. Avaya SIP Endpoint

- The standard SIP phone has about 30 basic telephony features but Avaya SIP endpoints are quite special.
- They have the ability to access the more than 700 Avaya Communication Manager features!
- So how does an Avaya SIP phone access telephony features when it now registers directly to Session Manager and is primarily routed by Session Manager?

bridged appearances

call forward

CM SIP Phone

SIP Phone

abbreviated dialing

mwi

call coverage

ec500

send-calls

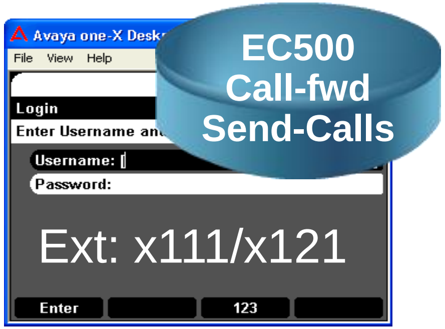
AVAYA | LEARNING

Let’s Add Some SIP Users!

Walk Through – User Profile for x111/x121

Step	Action
1	At System Manager console select User Management Menu
2	Select **New**
3	**<u>On the Identity Tab:</u>** • Add First/Last Name: Your name • Login Name: email address format i.e. **yourname@avaya.com** • Password: alpha-numeric format. 7 digit minimum i.e. **abc1234**
4	**<u>On the Communication Profile Tab:</u>** Password: Enter **123456** • Go down to Communication Address • Select New • Type: Avaya SIP • Fully qualified address : Student a = x111@training.com Student b = x121@training.com **Select Add**
5	**<u>Session Manager Profile</u>** Assign the user to your assigned Session Manager Origination and Termination Application Sequences: Select your CM Location: Denver
6	**<u>Endpoint Profile</u>** Select the CM and check "use existing endpoint". Select your station from the list, or type it. Let everything else default – except the Security Code. Enter '123456'.
7	Commit your changes

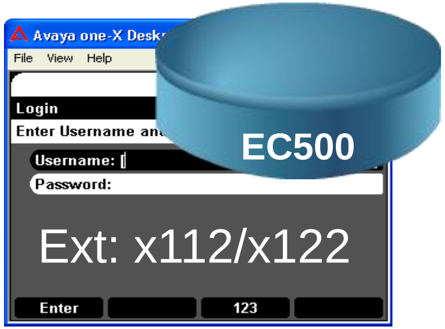
- Run traceSM to view the endpoint subscribe to CM event packages



Exercise: Create User Profile for x112/x122

Step	Action
1	At System Manager console select User Management Menu
2	Select **New**
3	**On the Identity Tab:** • Add First/Last Name: Your name • Login Name: email address format i.e. **yourname@avaya.com** • Password: alpha-numeric format. 7 digit minimum i.e. **abc1234**
4	**On the Communication Profile Tab:** Password: Enter **123456** • Go down to Communication Address • Select New • Type: Avaya SIP • Fully qualified address : Student a = x112@training.com Student b = x122@training.com **Select Add**
5	**Session Manager Profile** Assign the user to your assigned Session Manager Origination and Termination Application Sequences: Select your CM Location: Denver
6	**Endpoint Profile** Select the CM and check “use existing endpoint”. Select your station from the list, or type it. Let everything else default – except the Security Code. Enter ‘123456’.
7	Commit your changes

- Run traceSM to view the endpoint subscribe to CM event packages

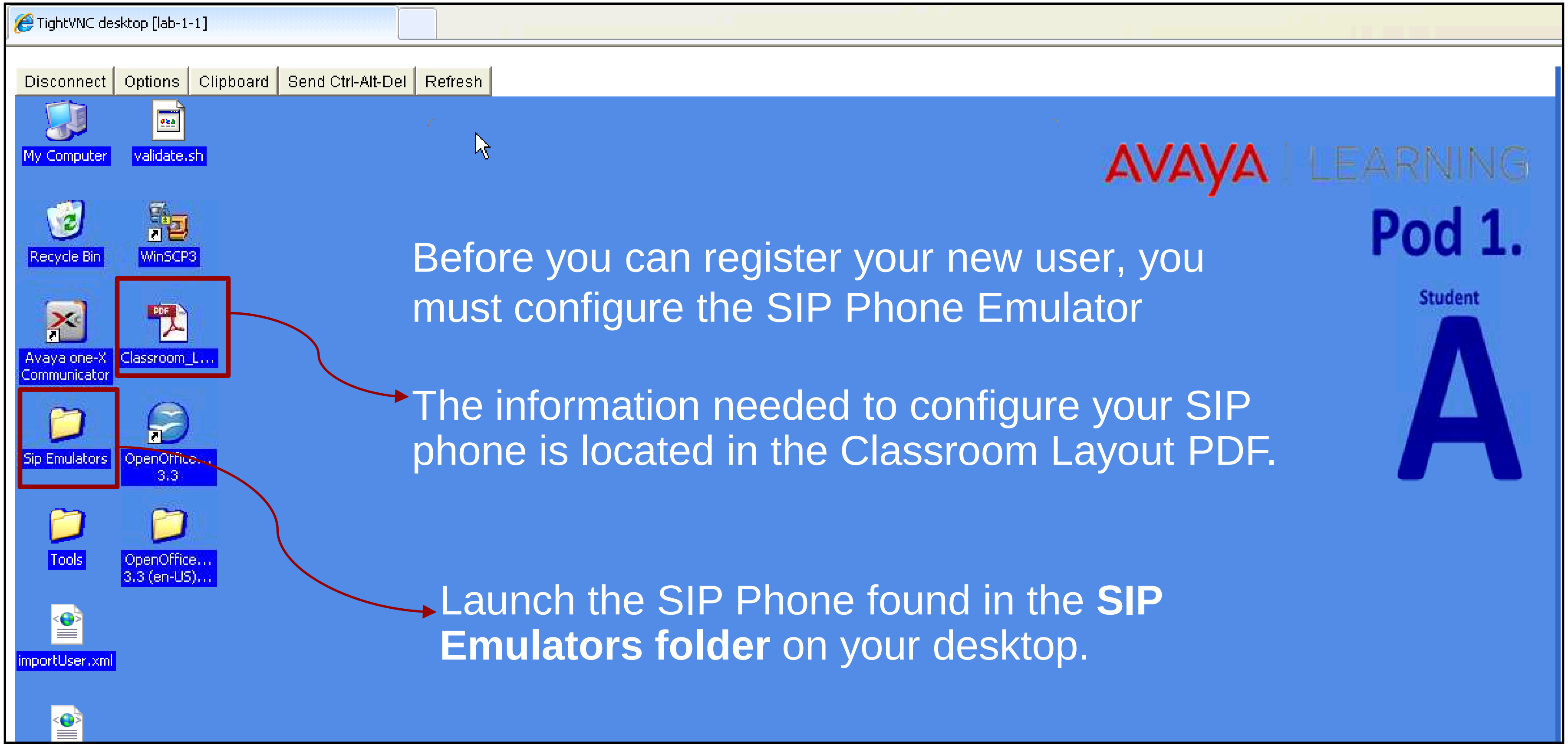


Exercise: Create User Profile for x113/x123

Step	Action
1	At System Manager console select User Management Menu
2	Select **New**
3	**<u>On the Identity Tab:</u>** • Add First/Last Name: Your name • Login Name: email address format i.e. **yourname@avaya.com** • Password: alpha-numeric format. 7 digit minimum i.e. **abc1234**
4	**<u>On the Communication Profile Tab:</u>** Password: Enter **123456** • Go down to Communication Address • Select New • Type: Avaya SIP • Fully qualified address : Student a = x113@training.com Student b = x123@training.com **Select Add**
5	**<u>Session Manager Profile</u>** Assign the user to your assigned Session Manager Origination and Termination Application Sequences: Select your CM Location: Denver
6	**<u>Endpoint Profile</u>** Select the CM and check "use existing endpoint". Select your station from the list, or type it. Let everything else default – except the Security Code. Enter '123456'.
7	Commit your changes

- Run traceSM to view the endpoint subscribe to CM event packages

The Next Exercise is a Review



Before you can register your new user, you must configure the SIP Phone Emulator

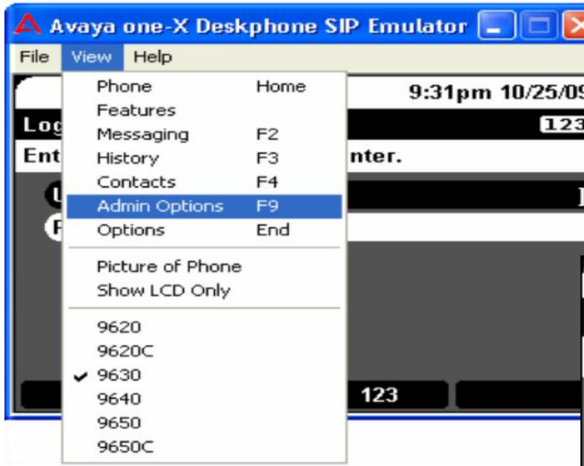
The information needed to configure your SIP phone is located in the Classroom Layout PDF.

Launch the SIP Phone found in the **SIP Emulators folder** on your desktop.

Exercise: Configure SIP Phones

- Open the **SIP Emulators Folder** on the Desktop

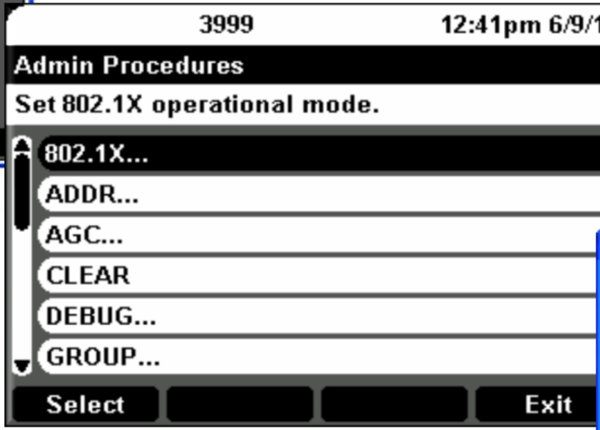
1. Navigate to ***View >> Admin Options***



*2. Select **ADDR** Menu*

Student a 172.16.x.11

Student b 172.16.x.12



3999 12:41pm 6/9/11

Admin Procedures

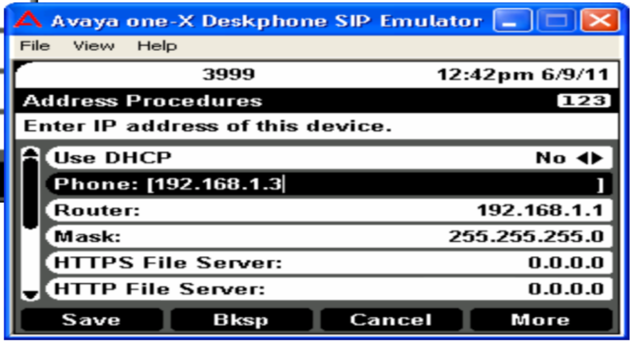
Set 802.1X operational mode.

3. Enter PC IP Addr:

***Router:** 172.16.255.254*

***Mask**: 255.255.0.0*

Save



3999 12:42pm 6/9/11

Address Procedures 123

Enter IP address of this device.

Use DHCP No

Phone: [192.168.1.3]

Router: 192.168.1.1

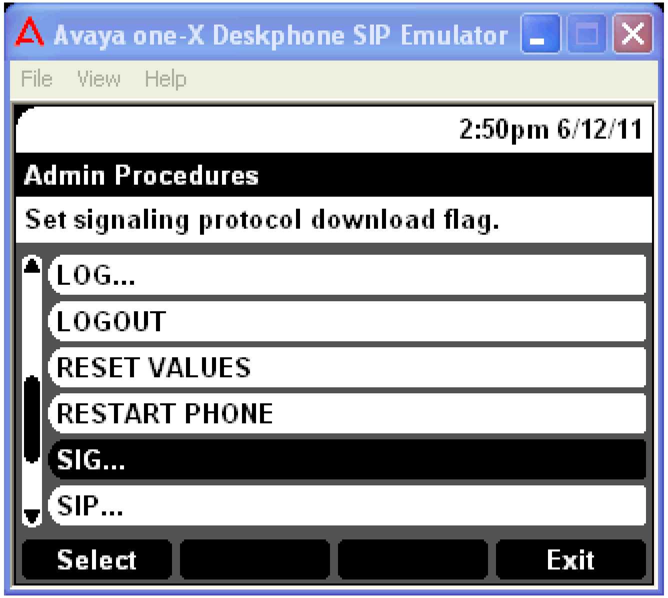
Mask: 255.255.255.0

HTTPS File Server: 0.0.0.0

HTTP File Server: 0.0.0.0

Exercise: Configure SIP Emulator (continued)

4. Select **SIG** Menu

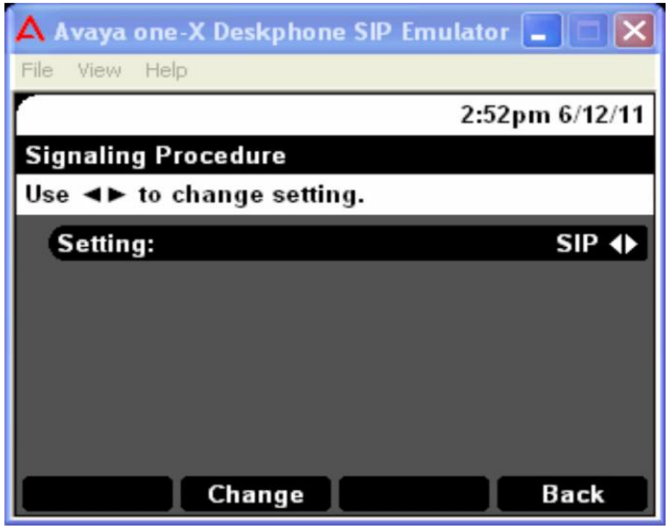


2:50pm 6/12/11

Admin Procedures

Set signaling protocol download flag.

5. Select the **SIP** Protocol: hit right arrow until SIP is selected and Save



2:52pm 6/12/11

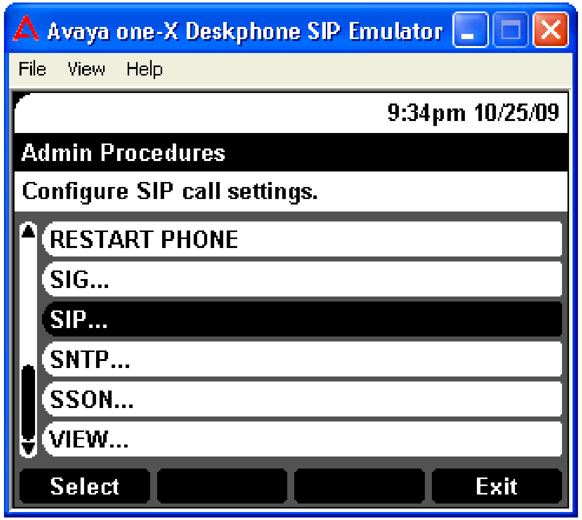
Signaling Procedure

Use ◄► to change setting.

Setting: SIP ◄►

Exercise: Configure SIP Emulator (continued)

6. Arrow down to **SIP** Menu



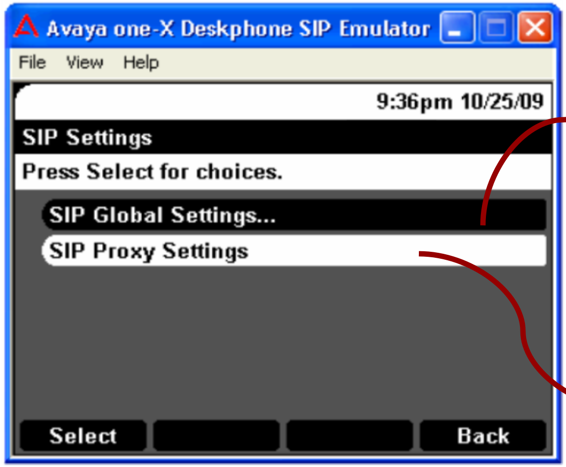
Avaya one-X Deskphone SIP Emulator

9:34pm 10/25/09

Admin Procedures

Configure SIP call settings.

7. Configure **SIP Global Settings**:
SIP Mode: Proxied
Domain: training.com

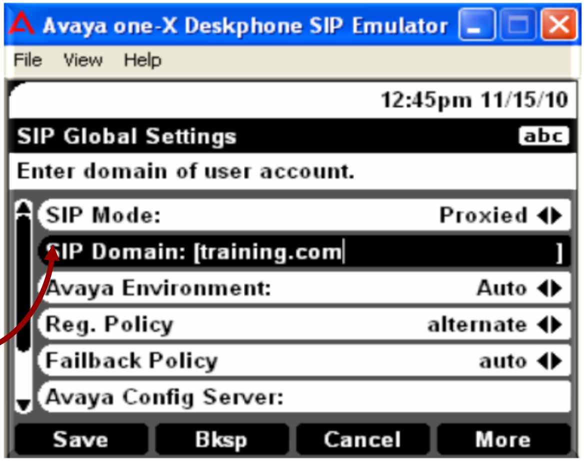


Avaya one-X Deskphone SIP Emulator

9:36pm 10/25/09

SIP Settings

Press Select for choices.



Avaya one-X Deskphone SIP Emulator

12:45pm 11/15/10

SIP Global Settings abc

Enter domain of user account.

SIP Mode: Proxied

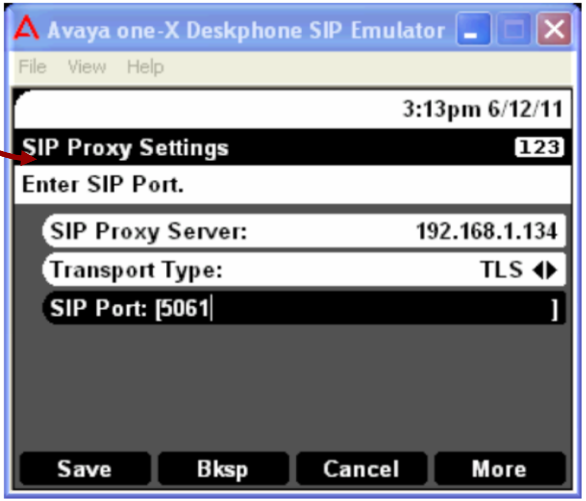
SIP Domain: [training.com]

Avaya Environment: Auto

Reg. Policy alternate

Failback Policy auto

Avaya Config Server:



Avaya one-X Deskphone SIP Emulator

3:13pm 6/12/11

SIP Proxy Settings 123

Enter SIP Port.

SIP Proxy Server: 192.168.1.134

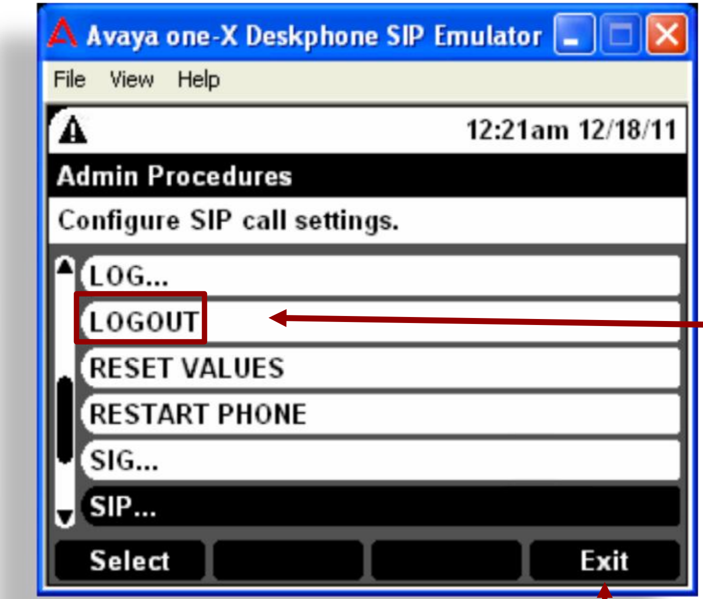
Transport Type: TLS

SIP Port: [5061]

8. Arrow down to **SIP Proxy Settings**:
SIP Proxy Server: 172.16.x.105
Transport Type: TLS
SIP Port: 5061

Exercise: Configure SIP Emulator (continued)

Do not select **EXIT**



Admin Procedures

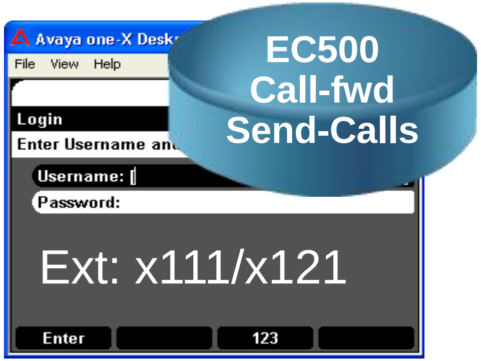
Configure SIP call settings.

Select
Logout
instead

Do Not Select EXIT and instead arrow UP to the Logout setting.
If you EXIT, the application will close and not retain your settings.

Exercise: Log in Using New User Profile – View Differences

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td><b>Access the SIP Phone Emulator folder and run three phones</b>
<table>
<tr><th>Student</th><th>Pod 1</th><th>Pod 2</th><th>Pod 3</th><th>Pod 4</th><th>Pod 5</th><th>Pod 6</th></tr>
<tr><td>Student a</td><td>1111
1112
1113</td><td>2111
2112
2113</td><td>3111
3112
3113</td><td>41114
11241
13</td><td>5111
5112
5113</td><td>6111
6112
6113</td></tr>
<tr><td>Student b</td><td>1121
1122
1123</td><td>2121
2122
2123</td><td>3121
3122
3123</td><td>41214
12241
23</td><td>5121
5122
5123</td><td>6121
6122
6123</td></tr>
</table>
Password: 123456</td></tr>
<tr><td>2</td><td>Log in as x111/x121, x112/x122 and x113/x123</td></tr>
<tr><td>3</td><td>Take time to review the SIP Trace</td></tr>
<tr><td>4</td><td>Select the SIP Phone with cursor.
Use the right arrow key on your keyboard to view features on SIP phone.</td></tr>
</table>



Login

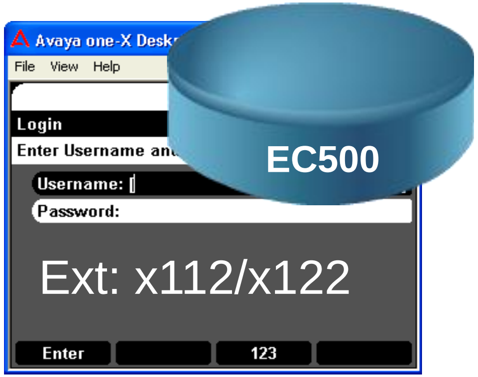
Enter Username an

Username:

Password:

EC500
Call-fwd
Send-Calls

Ext: x111/x121



Login

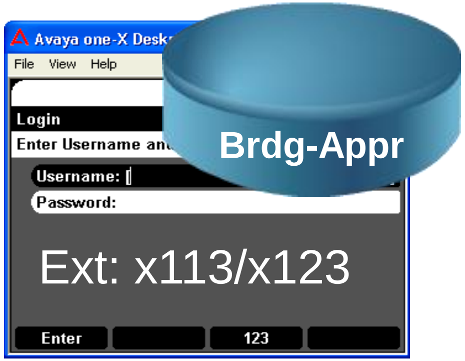
Enter Username an

Username:

Password:

EC500

Ext: x112/x122



Login

Enter Username an

Username:

Password:

Brdg-Appr

Ext: x113/x123

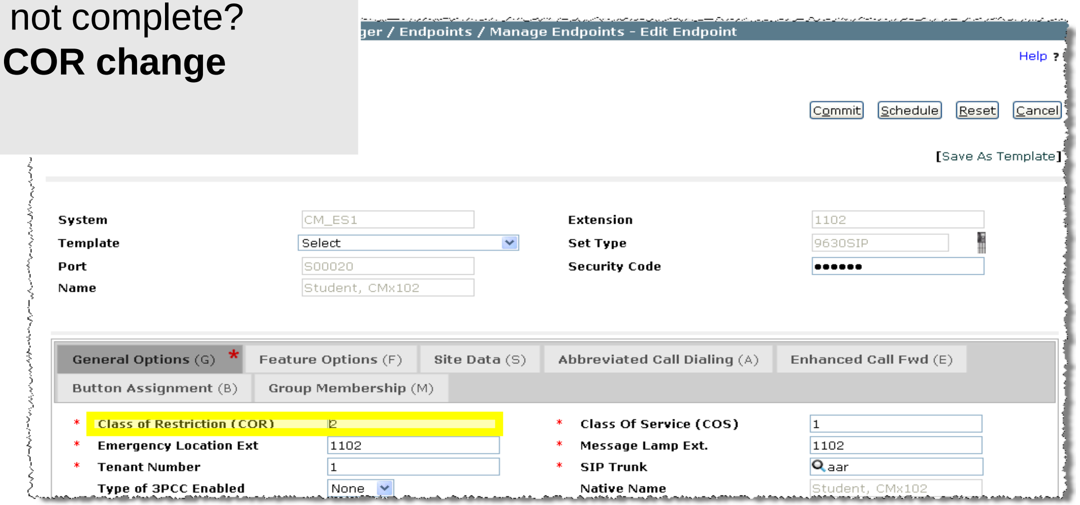
Exercise: Place a Call – x111/x121 dials x112/x122

Step	Action
1	Have your x111 SIP user call your x112 SIP user
2	Run traceSM
3	What did you observe when you selected the line to dial?
4	Observe the call path.
5	Did the call complete?
6	Did new headers get added to the request? What are they?

**hint: look for route headers in the SIP message*

Exercise: Place a Restricted Call

Step	Action
1	Have your x111 SIP user call your x112 SIP user
2	*In System Manager >> Communication Manager >> Endpoints >> Manage Endpoints,* Access x112 and change the Class of Restriction to '2' on the General Tab.
3	Run Incremental Sync
4	From x112, dial x111
5	Run traceSM
6	What was the reason the call did not complete? **Note: Make sure you undo the COR change before the next exercise *******



System	CM_ES1	Extension	1102
Template	Select	Set Type	9630SIP
Port	S00020	Security Code	●●●●●●
Name	Student, CMx102		

* Class of Restriction (COR)	2	* Class Of Service (COS)	1
* Emergency Location Ext	1102	* Message Lamp Ext.	1102
* Tenant Number	1	* SIP Trunk	aar
Type of 3PCC Enabled	None	Native Name	Student, CMx102

PPM – Personal Profile Manager

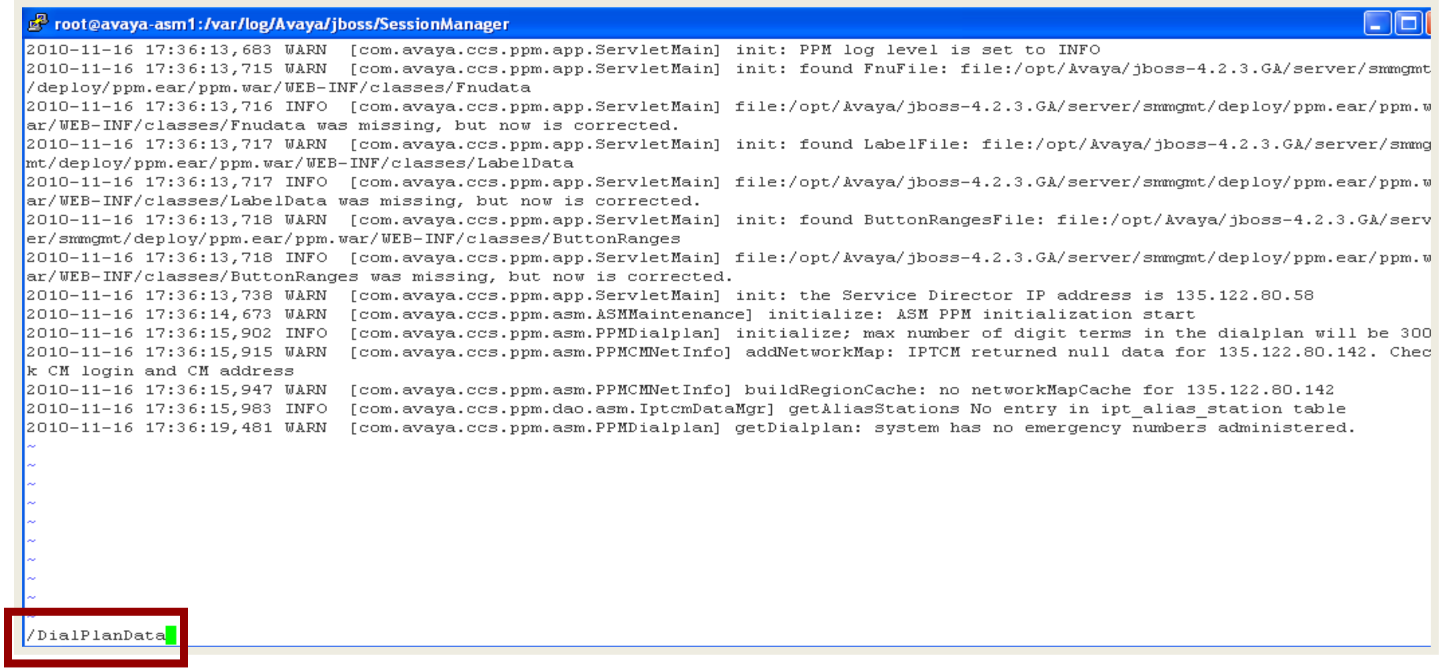
When a SIP phone registers to Session Manager, it is sent CM data such as button assignments, Dial Plan information, etc.

Activate/Deactivate PPM Logging

- enable PPM logging:
  - ***sm ppmlogon***
- To disable PPM logging:
  - ***sm ppmlogoff***

Verify User Login

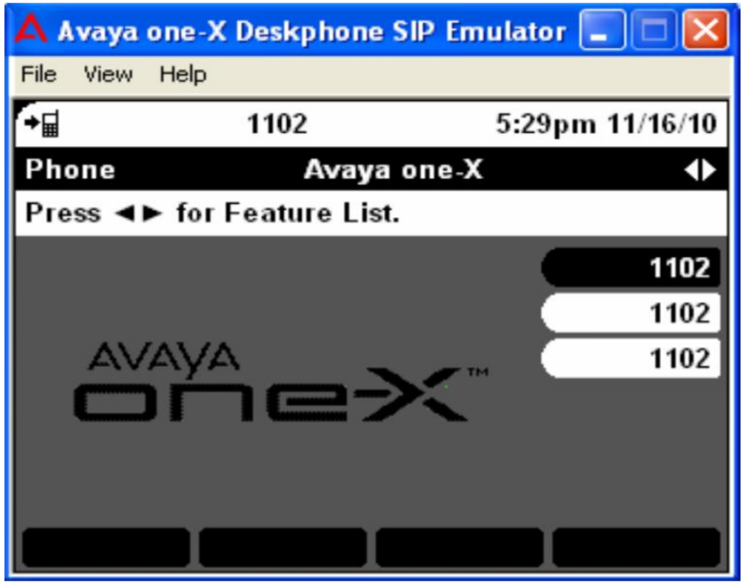
- To verify a user’s login and to view the data sent to the phone, log out a registered SIP phone – then re-login the same phone.
- On the Session Manager that the phone registers to:
  - **vi /var/log/Avaya/jboss/SessionManager/ppm.log**
    - go to bottom and search up for **DialPlanData**



```
2010-11-16 17:36:13,683 WARN  [com.avaya.ccs.ppm.app.ServletMain] init: PPM log level is set to INFO
2010-11-16 17:36:13,715 WARN  [com.avaya.ccs.ppm.app.ServletMain] init: found FnuFile: file:/opt/Avaya/jboss-4.2.3.GA/server/smmgmt
/deploy/ppm.ear/ppm.war/WEB-INF/classes/Fnudata
2010-11-16 17:36:13,716 INFO  [com.avaya.ccs.ppm.app.ServletMain] file:/opt/Avaya/jboss-4.2.3.GA/server/smmgmt/deploy/ppm.ear/ppm.w
ar/WEB-INF/classes/Fnudata was missing, but now is corrected.
2010-11-16 17:36:13,717 WARN  [com.avaya.ccs.ppm.app.ServletMain] init: found LabelFile: file:/opt/Avaya/jboss-4.2.3.GA/server/smmg
mt/deploy/ppm.ear/ppm.war/WEB-INF/classes/LabelData
2010-11-16 17:36:13,717 INFO  [com.avaya.ccs.ppm.app.ServletMain] file:/opt/Avaya/jboss-4.2.3.GA/server/smmgmt/deploy/ppm.ear/ppm.w
ar/WEB-INF/classes/LabelData was missing, but now is corrected.
2010-11-16 17:36:13,718 WARN  [com.avaya.ccs.ppm.app.ServletMain] init: found ButtonRangesFile: file:/opt/Avaya/jboss-4.2.3.GA/serv
er/smmgmt/deploy/ppm.ear/ppm.war/WEB-INF/classes/ButtonRanges
2010-11-16 17:36:13,718 INFO  [com.avaya.ccs.ppm.app.ServletMain] file:/opt/Avaya/jboss-4.2.3.GA/server/smmgmt/deploy/ppm.ear/ppm.w
ar/WEB-INF/classes/ButtonRanges was missing, but now is corrected.
2010-11-16 17:36:13,738 WARN  [com.avaya.ccs.ppm.app.ServletMain] init: the Service Director IP address is 135.122.80.58
2010-11-16 17:36:14,673 WARN  [com.avaya.ccs.ppm.asm.ASMMaintenance] initialize: ASM PPM initialization start
2010-11-16 17:36:15,902 INFO  [com.avaya.ccs.ppm.asm.PPMDialplan] initialize; max number of digit terms in the dialplan will be 300
2010-11-16 17:36:15,915 WARN  [com.avaya.ccs.ppm.asm.PPMCMNetInfo] addNetworkMap: IPTCM returned null data for 135.122.80.142. Chec
k CM login and CM address
2010-11-16 17:36:15,947 WARN  [com.avaya.ccs.ppm.asm.PPMCMNetInfo] buildRegionCache: no networkMapCache for 135.122.80.142
2010-11-16 17:36:15,983 INFO  [com.avaya.ccs.ppm.dao.asm.IptcmDataMgr] getAliasStations No entry in ipt_alias_station table
2010-11-16 17:36:19,481 WARN  [com.avaya.ccs.ppm.asm.PPMDialplan] getDialplan: system has no emergency numbers administered.
~
~
~
~
~
~
~
~
~
~
/DialPlanData
```

Exercise: Enable PPM.log

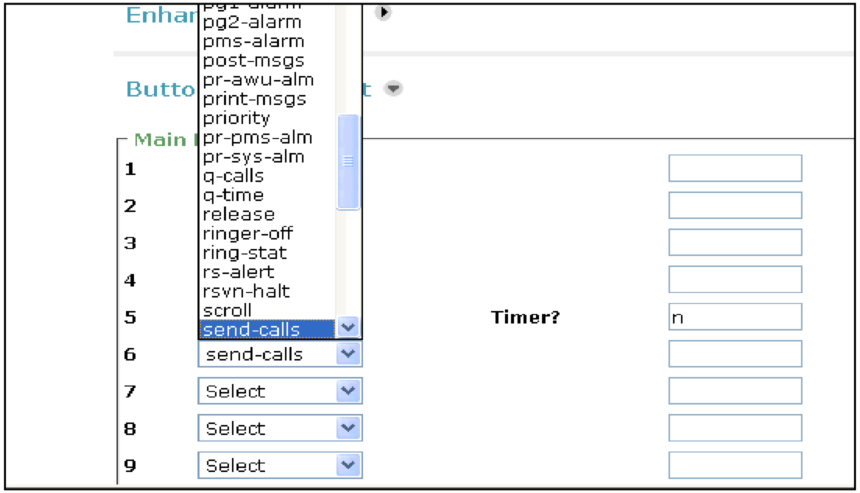
Step	Action
1	From the Session Manager Command Line type: **sm ppmlogon**
2	Logoff x112
3	Logon x112
4	Type: **vi/var/log/Avaya/jboss/SessionManager/ppm.log**
5	Type: **/DialPlanData**
6	To quit, type **:q!**



Exercise: Add Send – Calls Button Assignment

- Objective: Exercise will demonstrate CM can be used for managing endpoints.

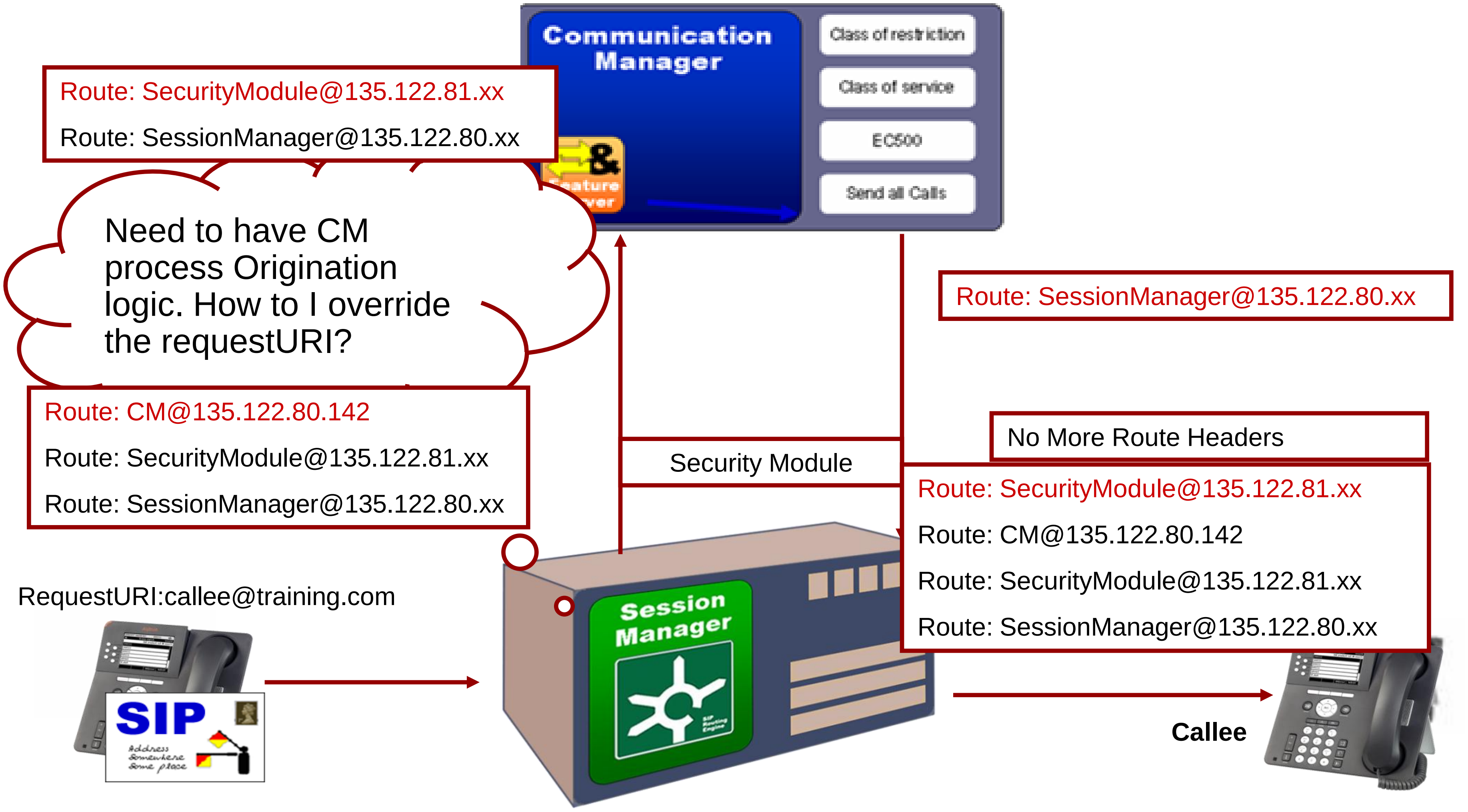
Step	Action
1	Go to Communication Manager Menu from Elements Menu
2	Go to Endpoints → Manage Endpoints
3	Edit station x112/x122.
	Under Button Assignment, select **Send-Calls** in drop-down. Leave the extension blank.
4	Save the Station.
5	Log on to station x112/x122 on the SIP Phone. View the phone features.



AVAYA | LEARNING

Sequenced Applications and Communication Manager

Half Call Model Route Headers



Route: SecurityModule@135.122.81.xx

Route: SessionManager@135.122.80.xx

Need to have CM process Origination logic. How to I override the requestURI?

Route: CM@135.122.80.142

Route: SecurityModule@135.122.81.xx

Route: SessionManager@135.122.80.xx

RequestURI:callee@training.com

Security Module

Route: SessionManager@135.122.80.xx

No More Route Headers

Route: SecurityModule@135.122.81.xx

Route: CM@135.122.80.142

Route: SecurityModule@135.122.81.xx

Route: SessionManager@135.122.80.xx

Callee

CM – Different Modes

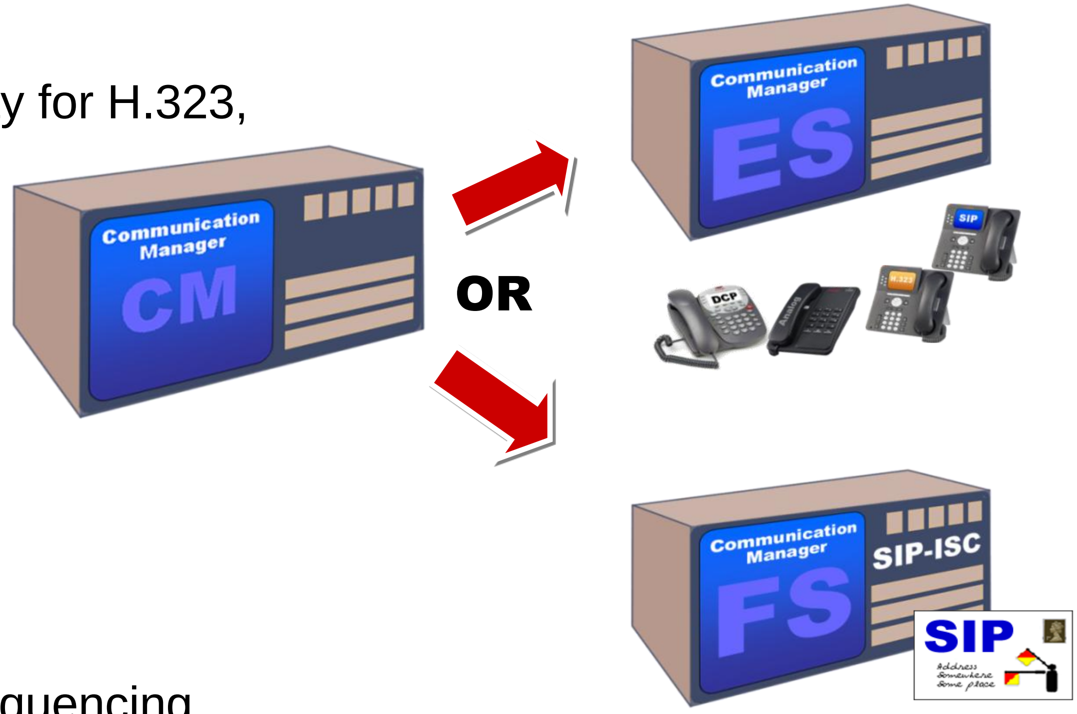
- While CM-FS is based on the half-call model, CM-ES is based on the traditional call model (a “modified” traditional call model).

CM-Evolution Server

- Access Point
- Acts as Access Point SIP Entity for H.323, DCP & Analog endpoints
- Supports SIP endpoints
- Supports all CM Trunk Types

Limited Application Sequencing

- ‘Full Call’ model



CM-Feature Server

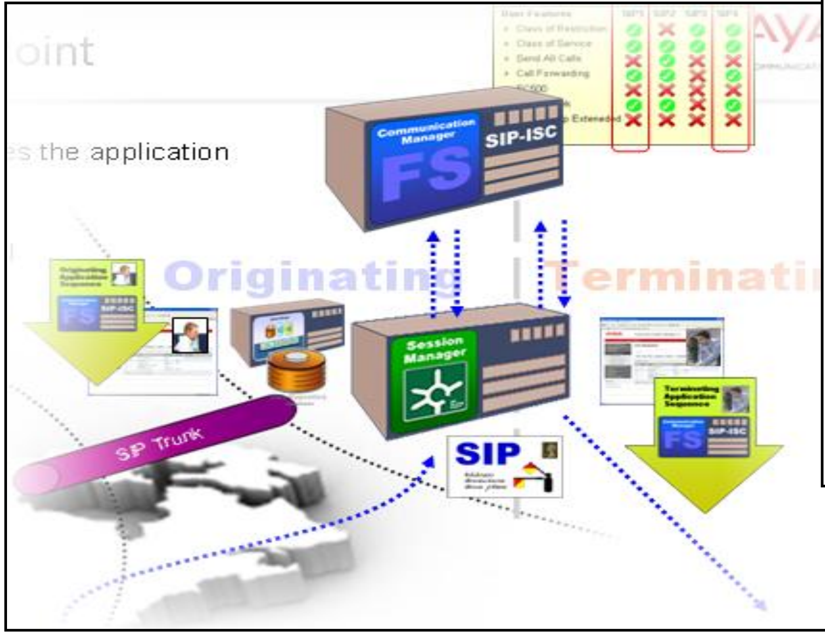
IMS type feature server

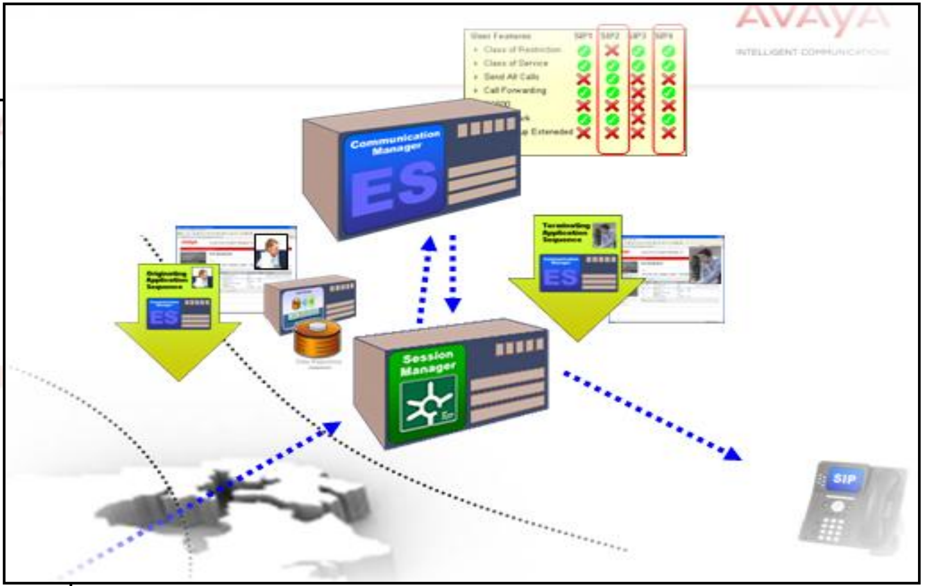
- Half Call Model Application Sequencing

Only SIP Endpoint Signaling Supported

CM-ES & CM-FS as Feature Server – Difference?

CM-FS: Half Call Model

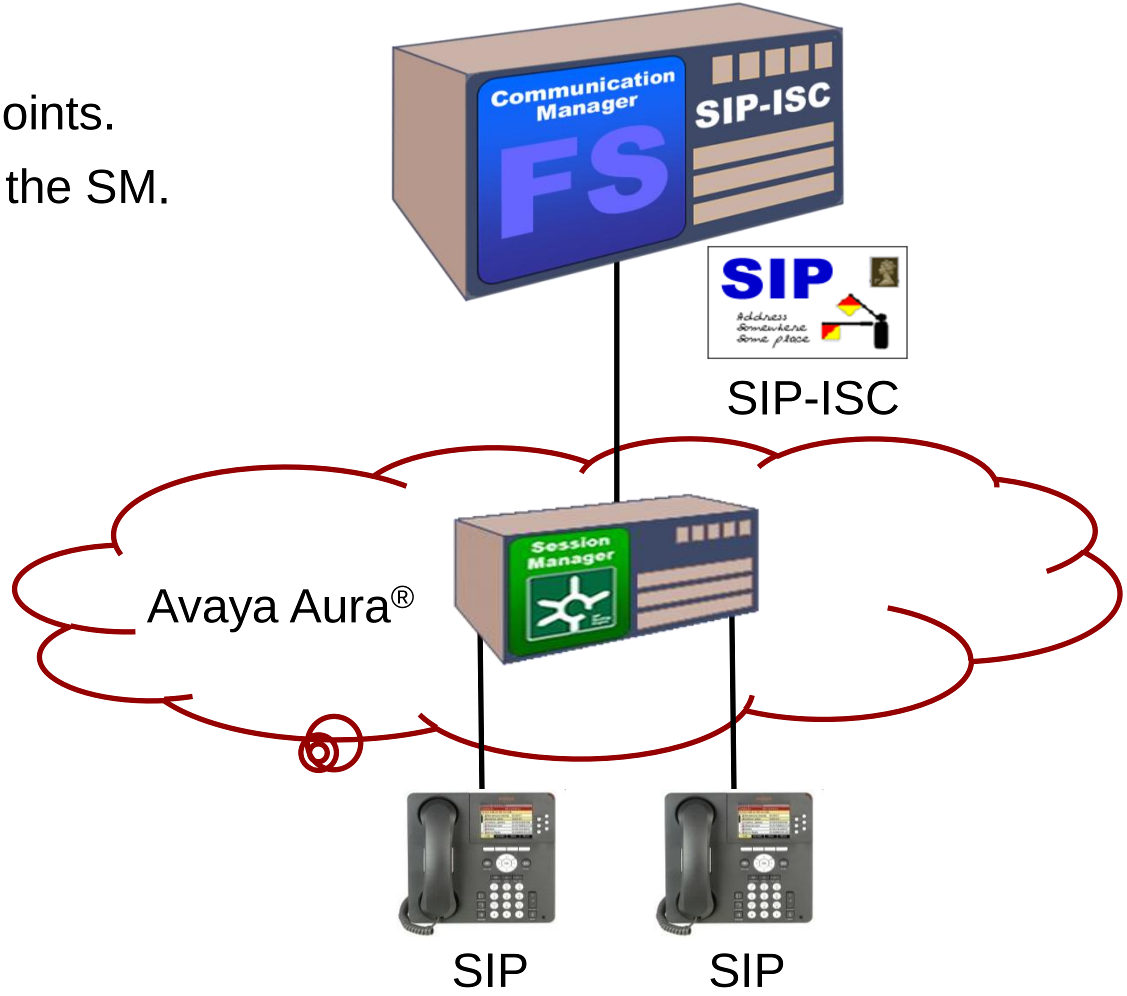




CM-ES: Full Call Model

CM as Feature Server (CM-FS)

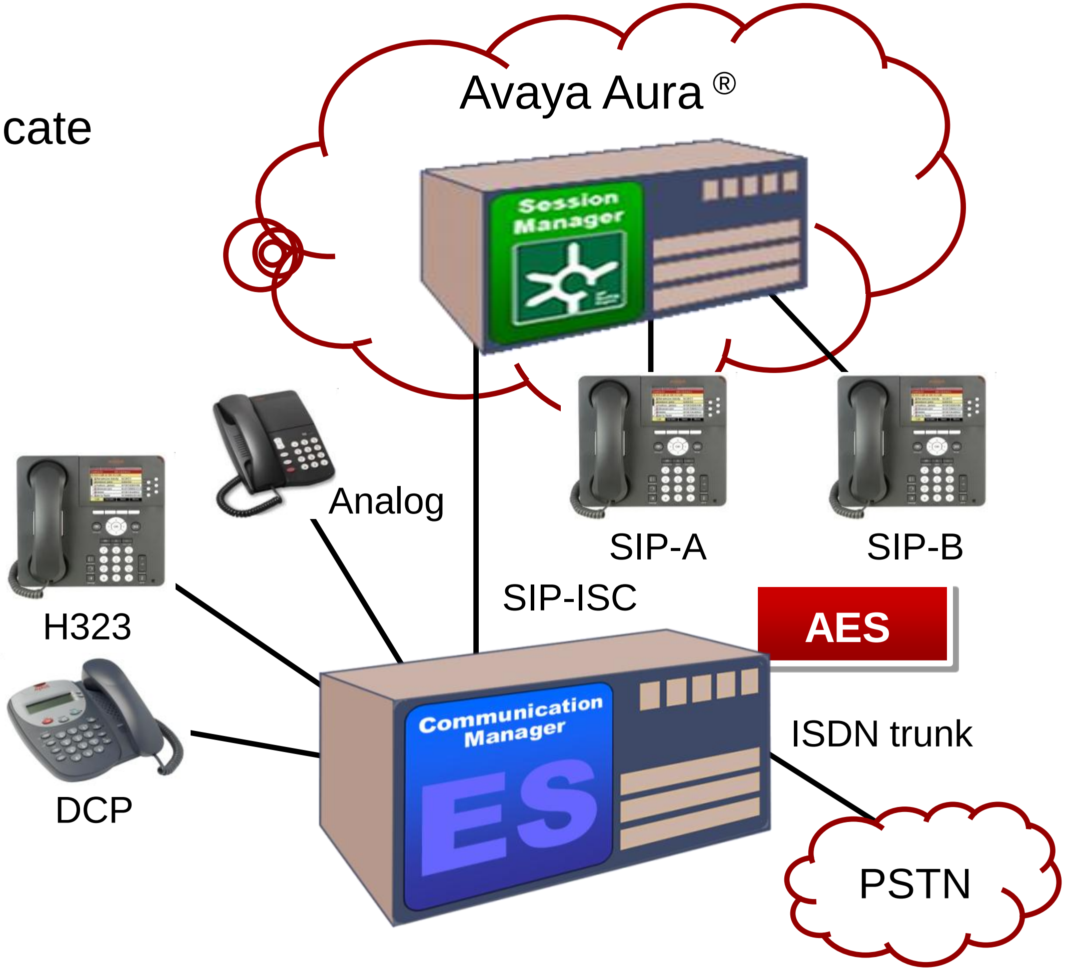
- CM is connected to the SM via a SIP-ISC interface.
- Half call model is required.
- CM only supports SIP endpoints.
- Calls are always routed via the SM.



CM as Evolution Server (CM-ES)

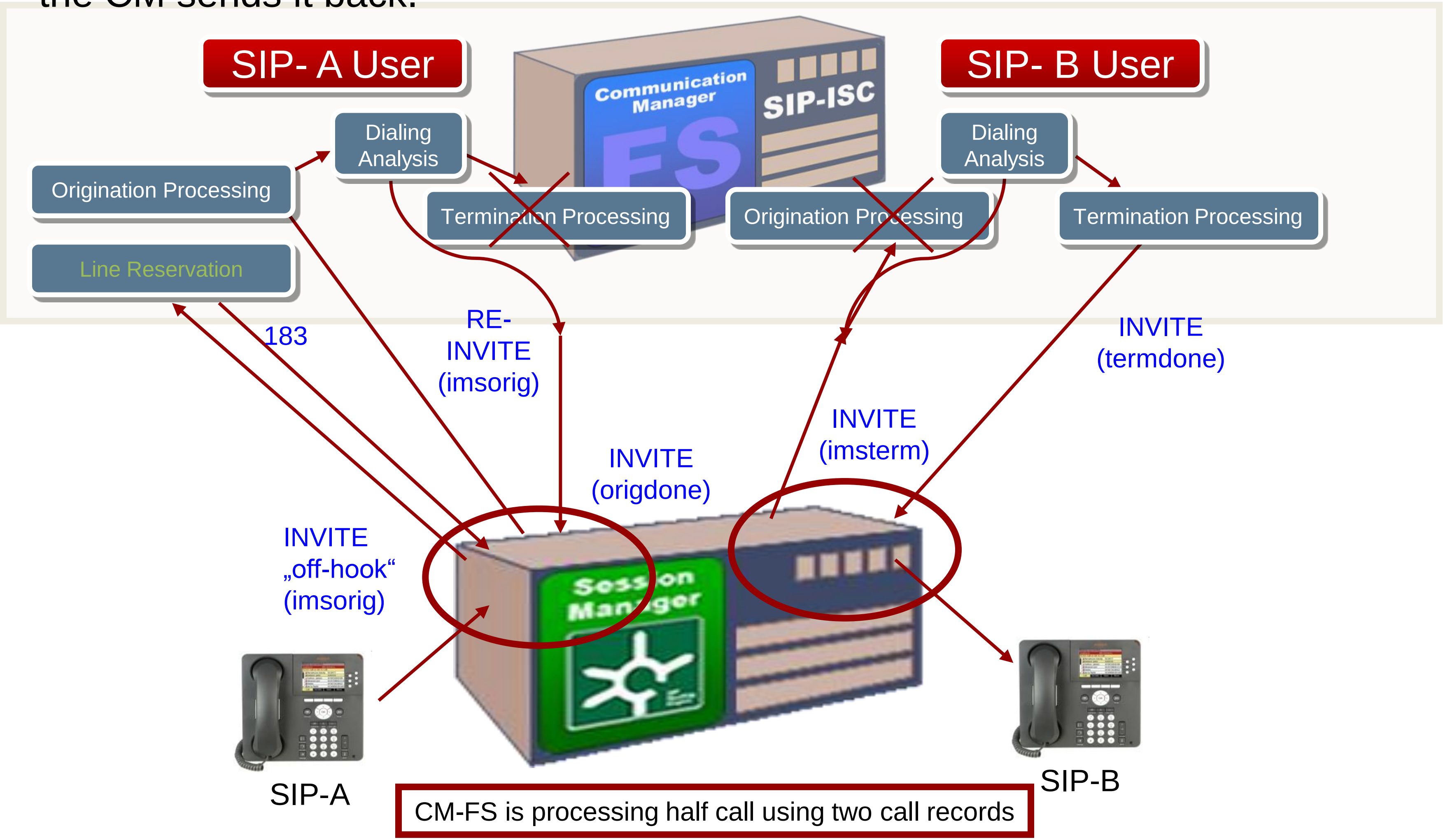
- CM is connected to the SM via a SIP-ISC interface.
- Full call model is required.
- SIP endpoints can communicate with all other endpoints.
- Calls from/to SIP endpoints are routed via the SM.

Comparing CM-ES with Classic-CM, Classic-CM integrates with Session Manager using the traditional SIP trunk interface, CM-ES allows the traditional SIP trunk as well as the SIP-ISC interface. Classic-CM supports SIP endpoints using SES, while CM-ES supports SIP endpoints using SM.



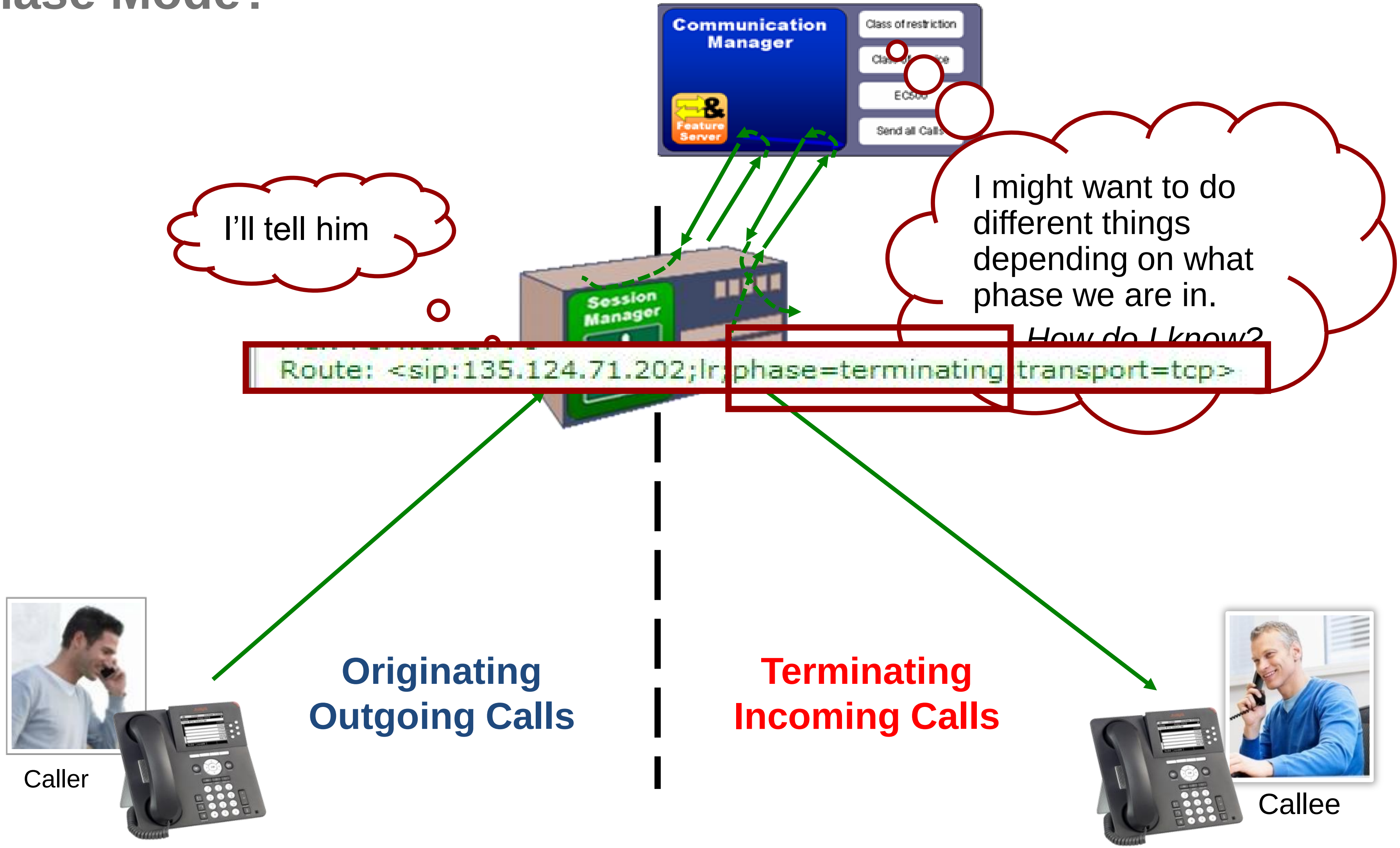
Half Call Principle – CM-FS

- The Session Manager will add route headers so the message is sent to CM and the CM sends it back.



CM-FS is processing half call using two call records

Phase Mode?



```
Route: <sip:135.124.71.202;lr;phase=terminating;transport=tcp>
```

Originating Outgoing Calls

Terminating Incoming Calls

Example of Phase Tags Options

Destination: user in the Request URI

Originator: user in P-Asserted ID header

Phase tags are added into the route header.

- imsorig: added by Session Manager to request origination side processing
- origdone: added by URE to its own route header to indicate Origination side processing done
- imsterm: added by Session Manager to request termination side processing
- termdone: added by URE to its own route header to indicate Termination side processing done

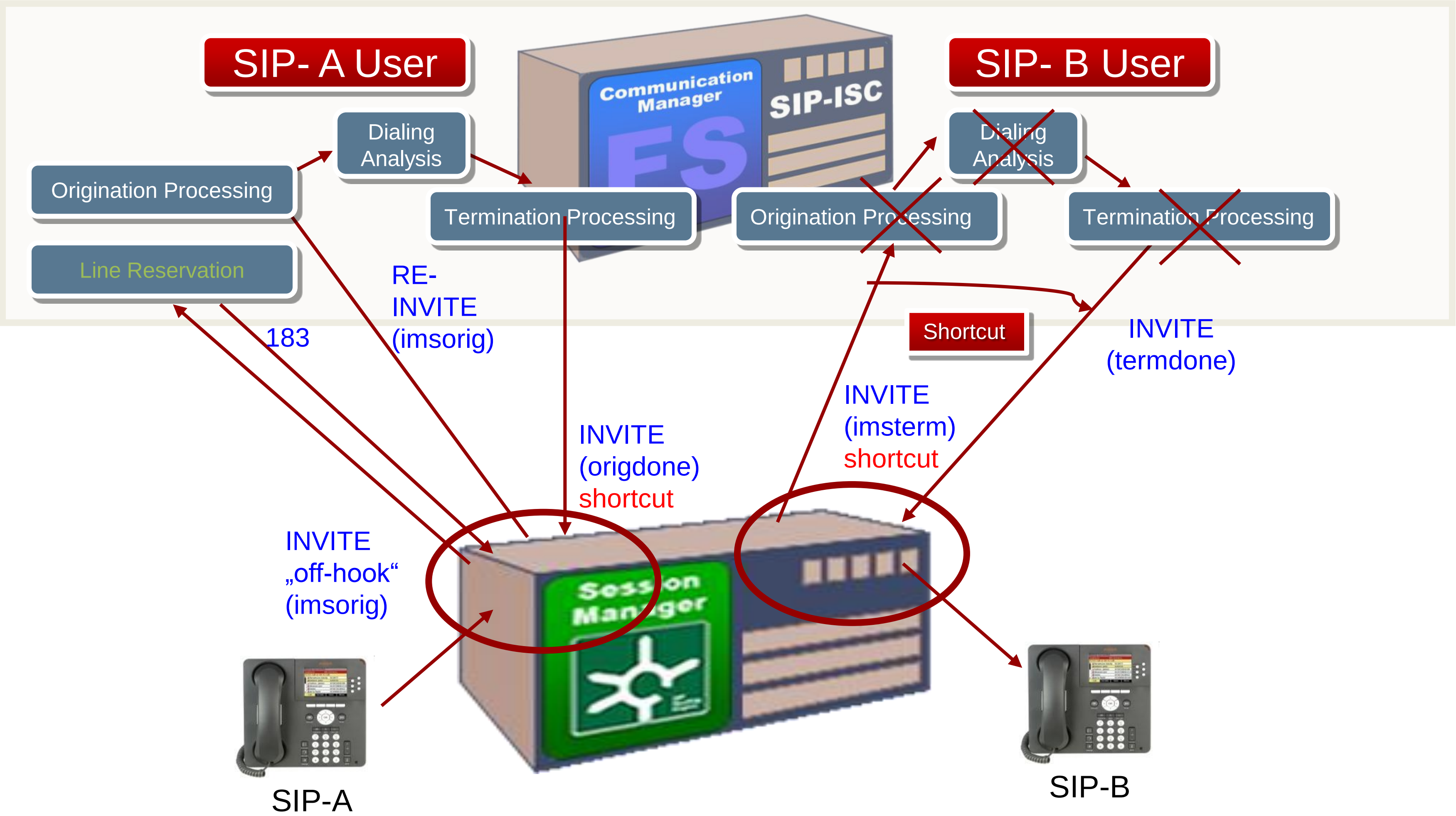
```
INVITE SIP:callee@avaya.com  SIP/2.0

To: Bill<SIP:bill@work.com>
From: John<SIP:john@home.com>
Call-ID: 267343@172.16.1.212
P-Asserted ID: caller@callersdomain.com
Route: appuri;lr;phase=imsorig
Route: asmuri;lr;phase=origdone
```

Full Call Principle – CM-ES

Upon receiving a request that contains an IMS Origination phase tag on a non-IMS signaling trunk, CM-ES will suppress the half-call model processing. It will perform the **originating AND terminating** side processing (the traditional call model) before forwarding the request back to Session Manager.

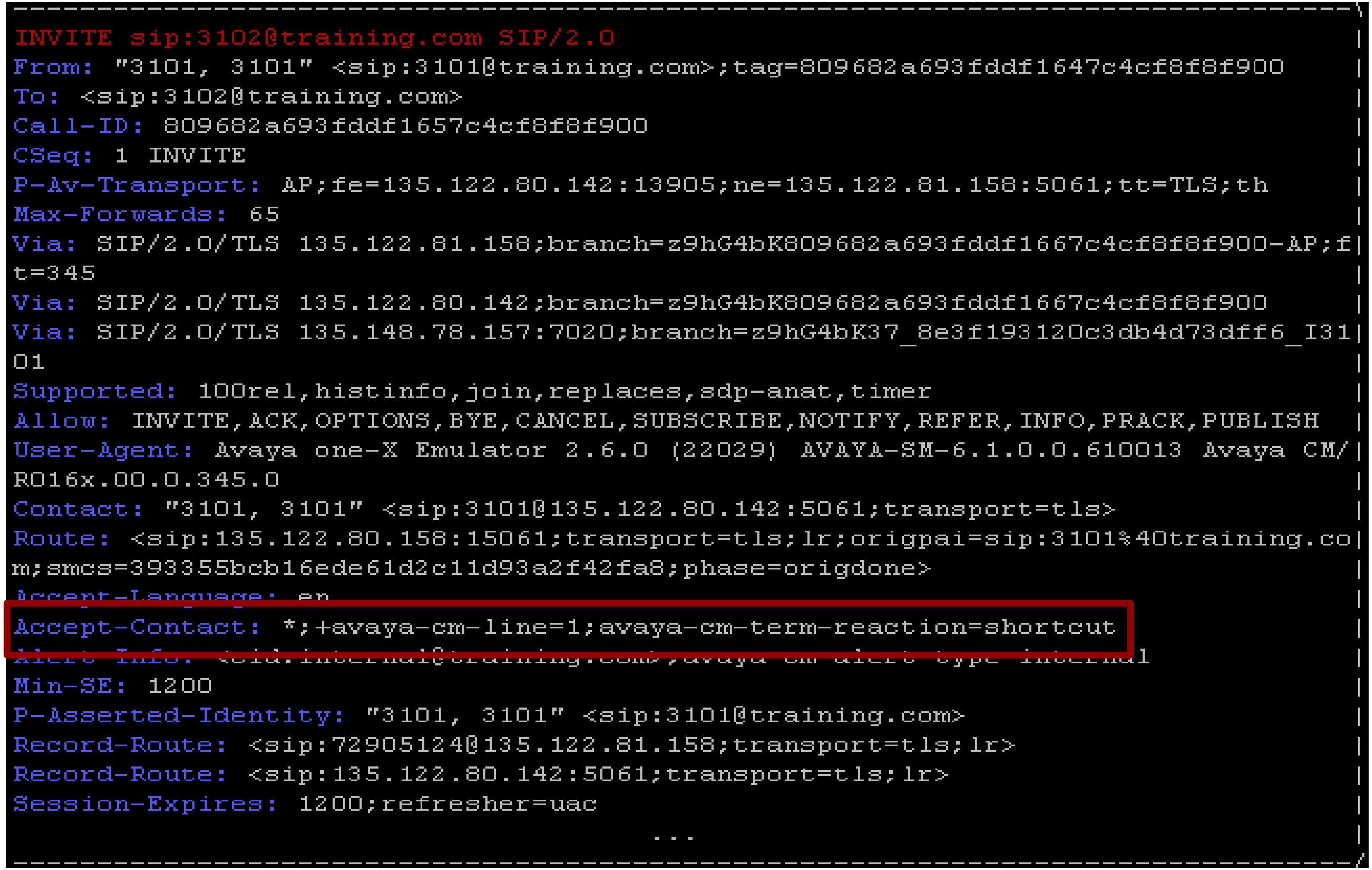
Traditional Call Processing

Full Call Principle – CM-ES (continued)



CM-ES is processing full call using one call record

CM-Evolution Server “shortcut” flag- avaya-cm-term-reaction



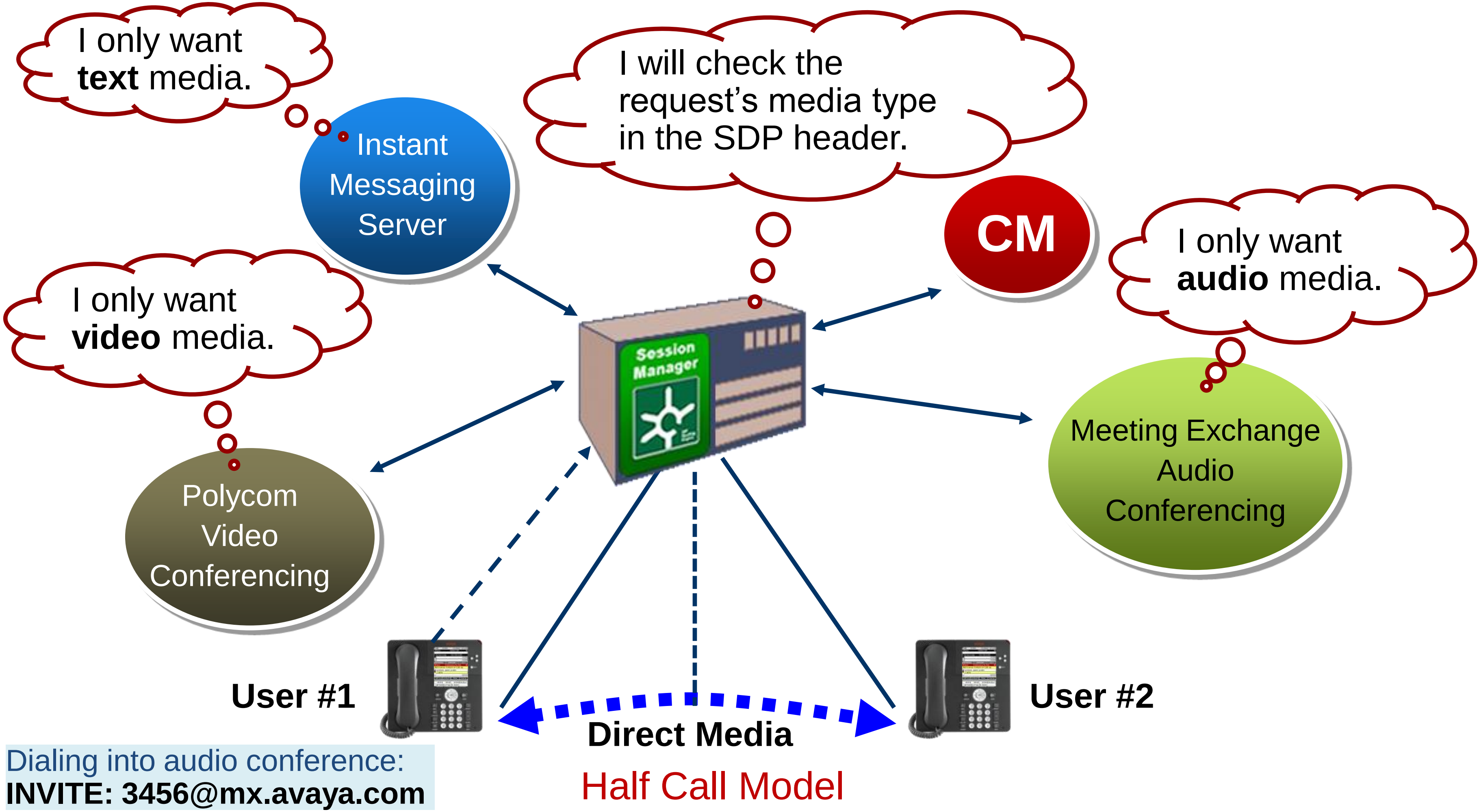
```
INVITE sip:3102@training.com SIP/2.0
From: "3101, 3101" <sip:3101@training.com>;tag=809682a693fddf1647c4cf8f8f900
To: <sip:3102@training.com>
Call-ID: 809682a693fddf1657c4cf8f8f900
CSeq: 1 INVITE
P-Av-Transport: AP;fe=135.122.80.142:13905;ne=135.122.81.158:5061;tt=TLS;th
Max-Forwards: 65
Via: SIP/2.0/TLS 135.122.81.158;branch=z9hG4bK809682a693fddf1667c4cf8f8f900-AP;f
t=345
Via: SIP/2.0/TLS 135.122.80.142;branch=z9hG4bK809682a693fddf1667c4cf8f8f900
Via: SIP/2.0/TLS 135.148.78.157:7020;branch=z9hG4bK37_8e3f193120c3db4d73dff6_I31
01
Supported: 100rel,histinfo,join,replaces,sdp-anat,timer
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,INFO,PRACK,PUBLISH
User-Agent: Avaya one-X Emulator 2.6.0 (22029) AVAYA-SM-6.1.0.0.610013 Avaya CM/
R016x.00.0.345.0
Contact: "3101, 3101" <sip:3101@135.122.80.142:5061;transport=tls>
Route: <sip:135.122.80.158:15061;transport=tls;lr;origpai=sip:3101%40training.co
m;smcs=393355bcb16ede61d2c11d93a2f42fa8;phase=origdone>
Accept-Language: en
Accept-Contact: *;+avaya-cm-line=1;avaya-cm-term-reaction=shortcut
Alert-Info: <cid:internal@training.com>;avaya-cm-alert-type=internal
Min-SE: 1200
P-Asserted-Identity: "3101, 3101" <sip:3101@training.com>
Record-Route: <sip:72905124@135.122.81.158;transport=tls;lr>
Record-Route: <sip:135.122.80.142:5061;transport=tls;lr>
Session-Expires: 1200;refresher=uac
                                        ...
```

AVAYA | LEARNING

Media-Filtered Application Sequencing

Media-Filtering new in 6.2

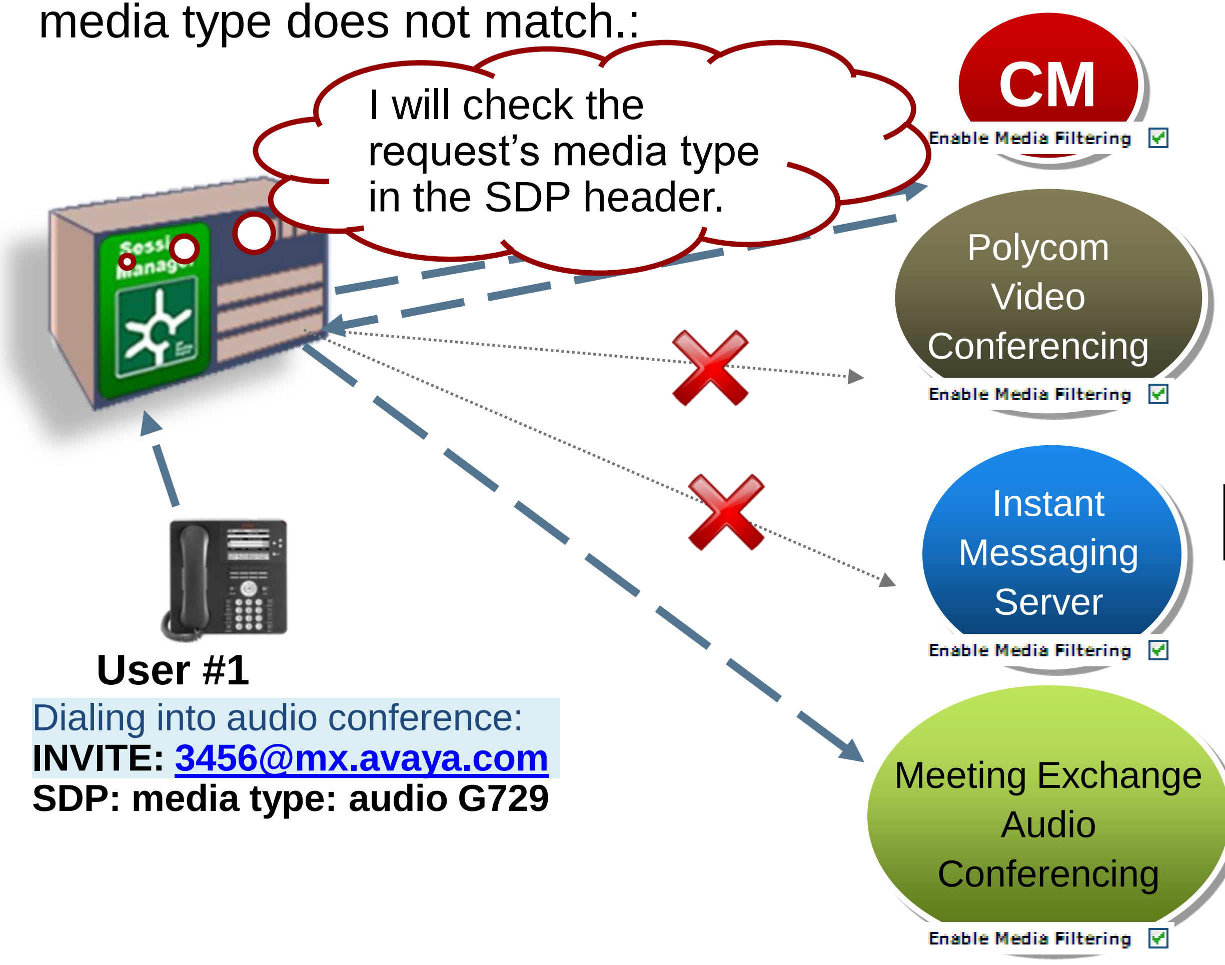
Session Manager can now route calls to applications based on the media type:
text, audio, video for more efficient and faster call processing.


I only want **text** media.
Instant Messaging Server
I will check the request's media type in the SDP header.
CM
I only want **audio** media.
I only want **video** media.
Session Manager
Meeting Exchange Audio Conferencing
Polycom Video Conferencing
User #1
User #2
Direct Media
Half Call Model

Dialing into audio conference:
INVITE: 3456@mx.avaya.com

Media-Filtering new in 6.2 (continued)

Session Manager will check the SDP media and based on the media-filtering configured in the applications , will skip the applications in the sequence for which the media type does not match.:



I will check the request’s media type in the SDP header.

CM

Enable Media Filtering ☑

Polycom Video Conferencing

Enable Media Filtering ☑

Instant Messaging Server

Enable Media Filtering ☑

Meeting Exchange Audio Conferencing

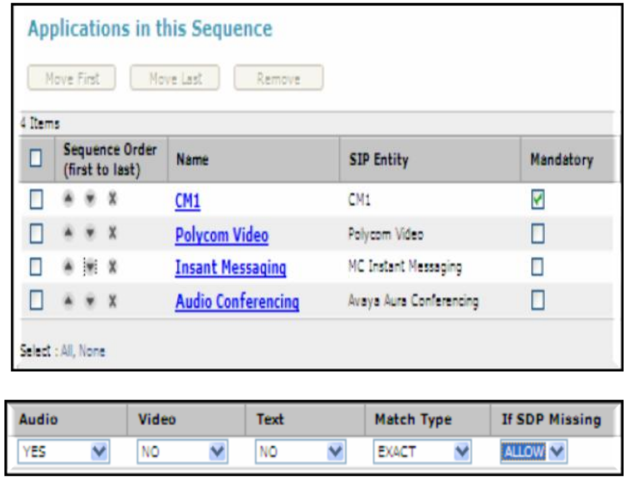
Enable Media Filtering ☑

User #1

Dialing into audio conference:

INVITE: 3456@mx.avaya.com

SDP: media type: audio G729



Applications in this Sequence

4 Items

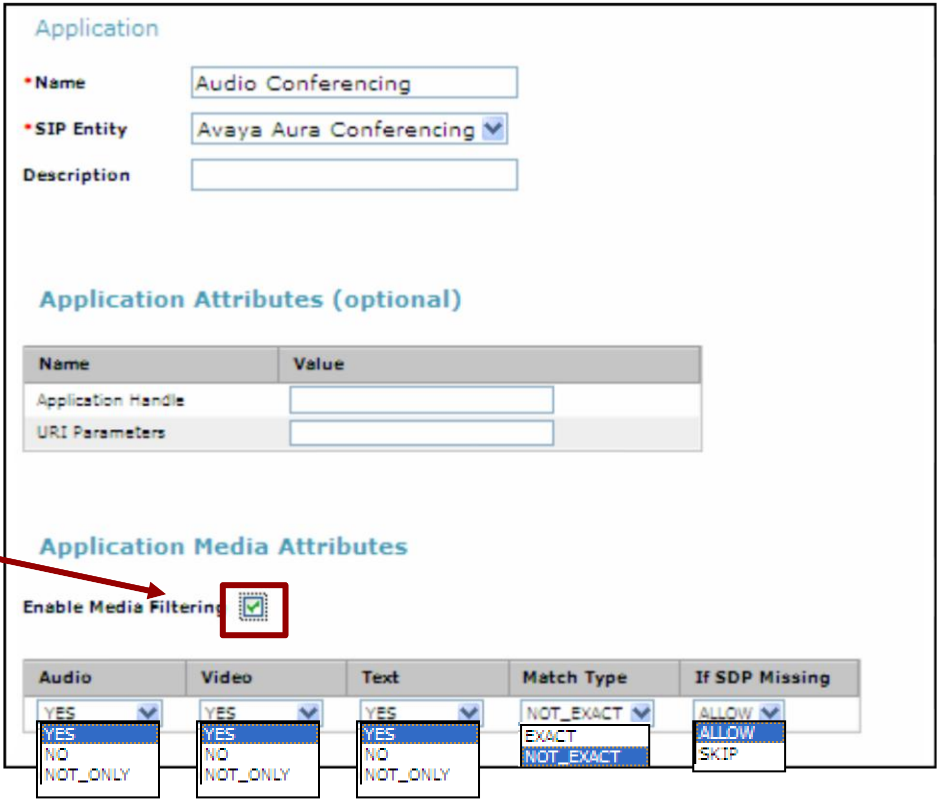
☐	Sequence Order (first to last)	Name	SIP Entity	Mandatory
☐	▲ ▼ X	CM1	CM1	☑
☐	▲ ▼ X	Polycom Video	Polycom Video	☐
☐	▲ ▼ X	Insant Messaging	MC Instant Messaging	☐
☐	▲ ▼ X	Audio Conferencing	Avaya Aura Conferencing	☐

Select : All, None

Audio	Video	Text	Match Type	If SDP Missing
YES	NO	NO	EXACT	ALLOW

Enabling Media-Filtering in Applications

From the Session Manager Menu, select Applications and edit the application.



Application

*Name	Audio Conferencing
*SIP Entity	Avaya Aura Conferencing
Description	

Application Attributes (optional)

Name	Value
Application Handle	
URI Parameters	

Application Media Attributes

Enable Media Filtering ☑

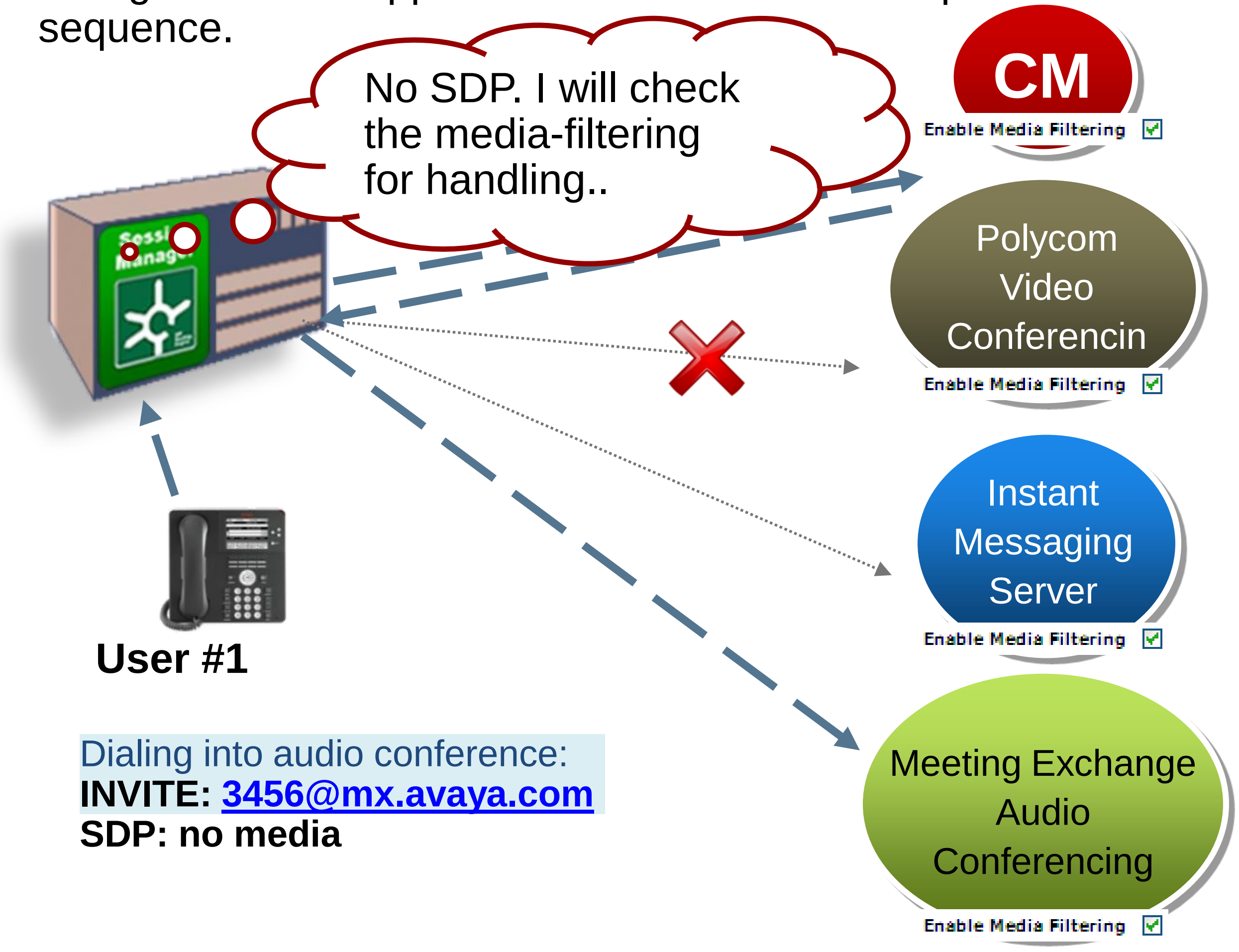
Audio	Video	Text	Match Type	If SDP Missing
YES	YES	YES	NOT_EXACT	ALLOW

Select the **Enable Media Filtering** box

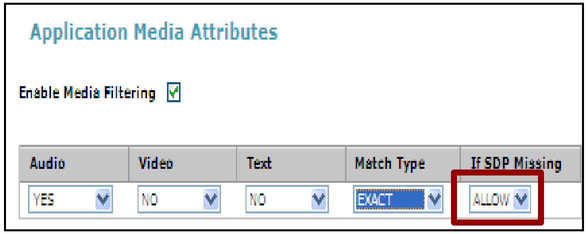
You can select which media type the application supports: audio, video, text.
You can match the exact combination or be more flexible by select NOT_Exact
You can even account for missing SDP header info.

Media-Filtering with No SDP Info

If Session Manager detects no SDP media defined in the packet it will check the **"If SDP Missing"** field in the Applications defined in the sequence. Based on the media-filtering configured in the applications ASM will either skip or allow routing to the applications in the sequence.



Dialing into audio conference:
INVITE: 3456@mx.avaya.com
SDP: no media



Application Media Attributes

Enable Media Filtering ☑

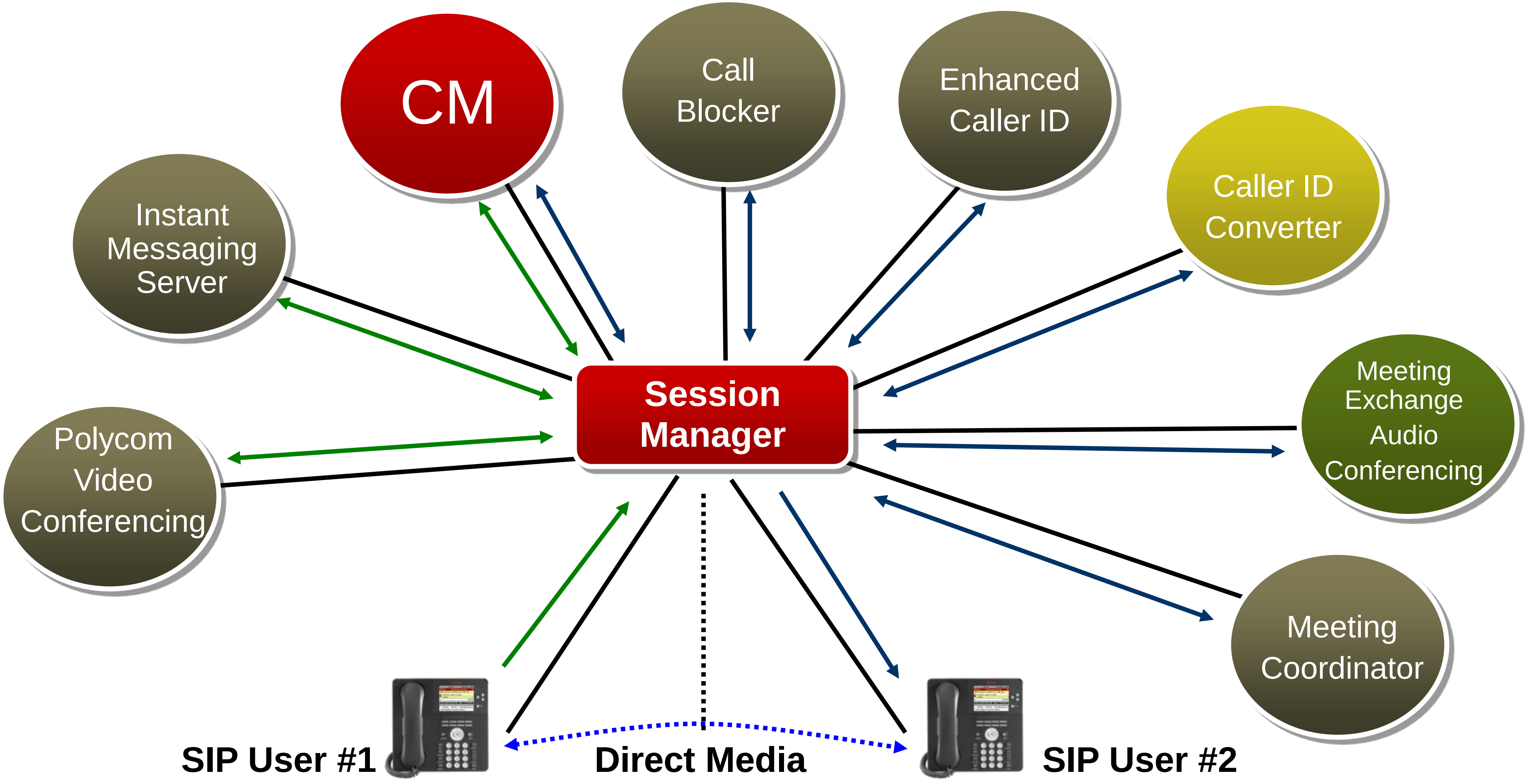
Audio	Video	Text	Match Type	If SDP Missing
YES	NO	NO	EXACT	ALLOW

AVAYA | LEARNING

Implementing 3rd Party Feature Server

Application Sequencing

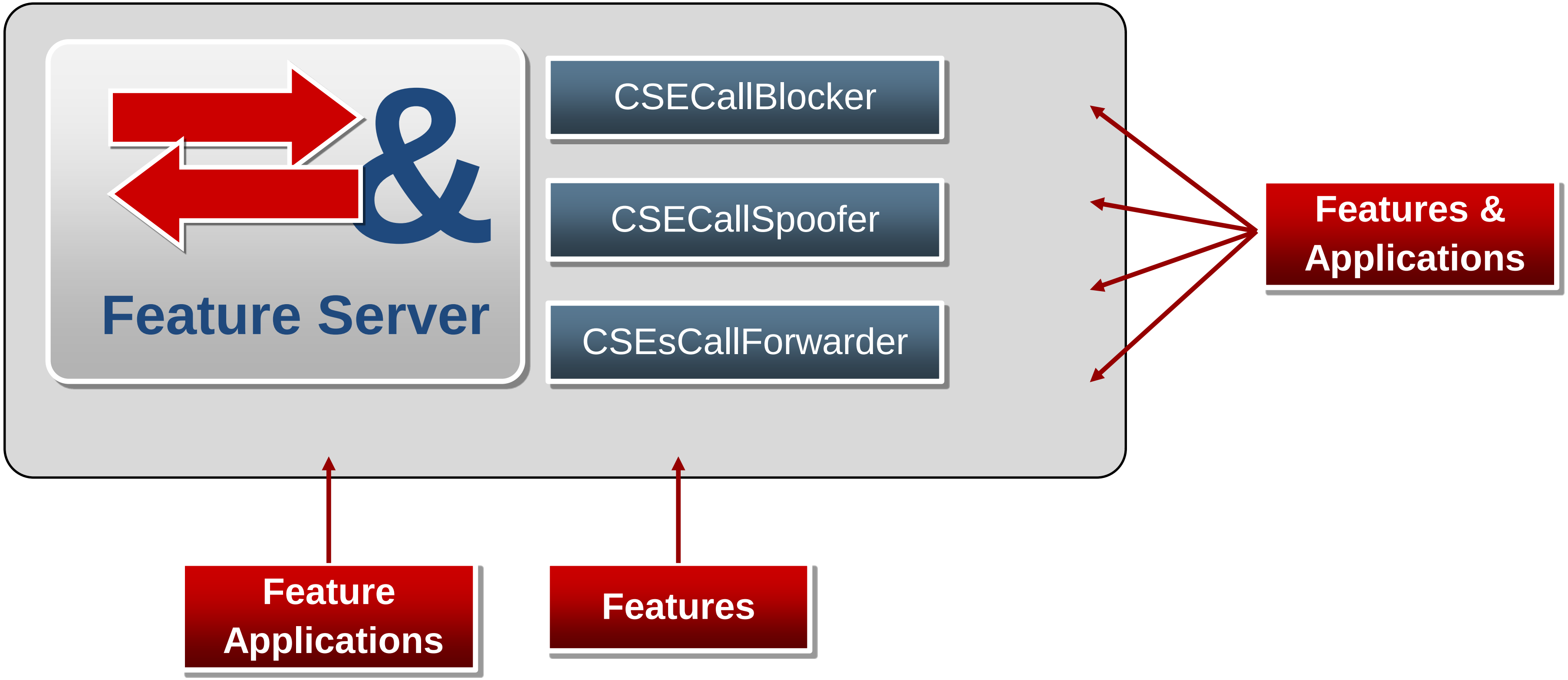
Avaya Aura^{TM} Sequenced Applications in an IMS Network



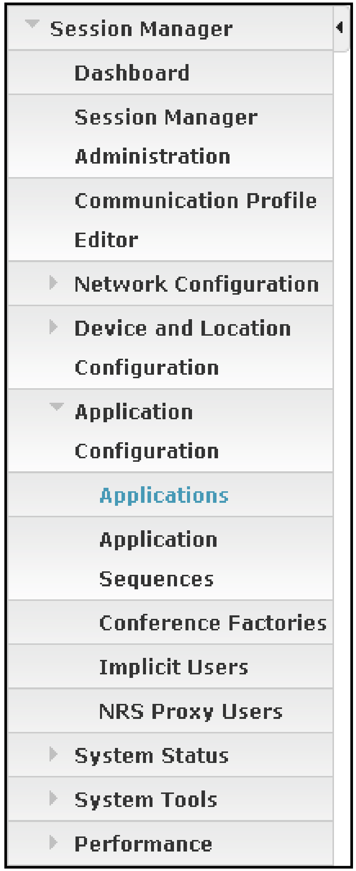
Half Call Model

Feature v. Feature Server

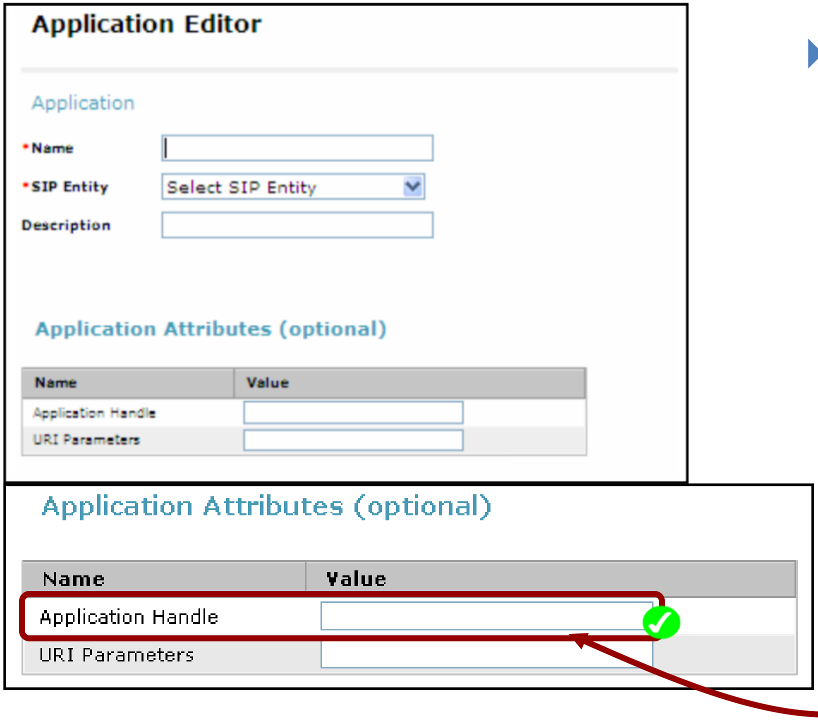
- 3rd party feature servers are configured differently than CM.
- One application can provide a variety of features.



Define the Application for 3rd Party Feature Server



- Session Manager
  - Dashboard
  - Session Manager Administration
  - Communication Profile Editor
  - Network Configuration
  - Device and Location Configuration
  - Application Configuration
    - Applications
    - Application Sequences
    - Conference Factories
    - Implicit Users
    - NRS Proxy Users
  - System Status
  - System Tools
  - Performance



Application Editor

Application

*Name	
*SIP Entity	Select SIP Entity
Description	

Application Attributes (optional)

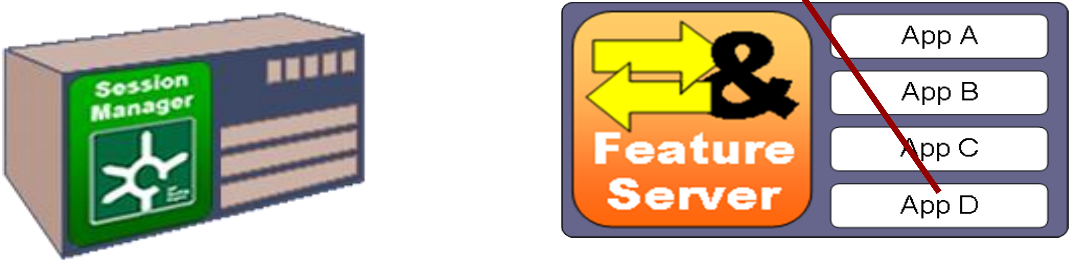
Name	Value
Application Handle	
URI Parameters	

Application Attributes (optional)

Name	Value
Application Handle	
URI Parameters	

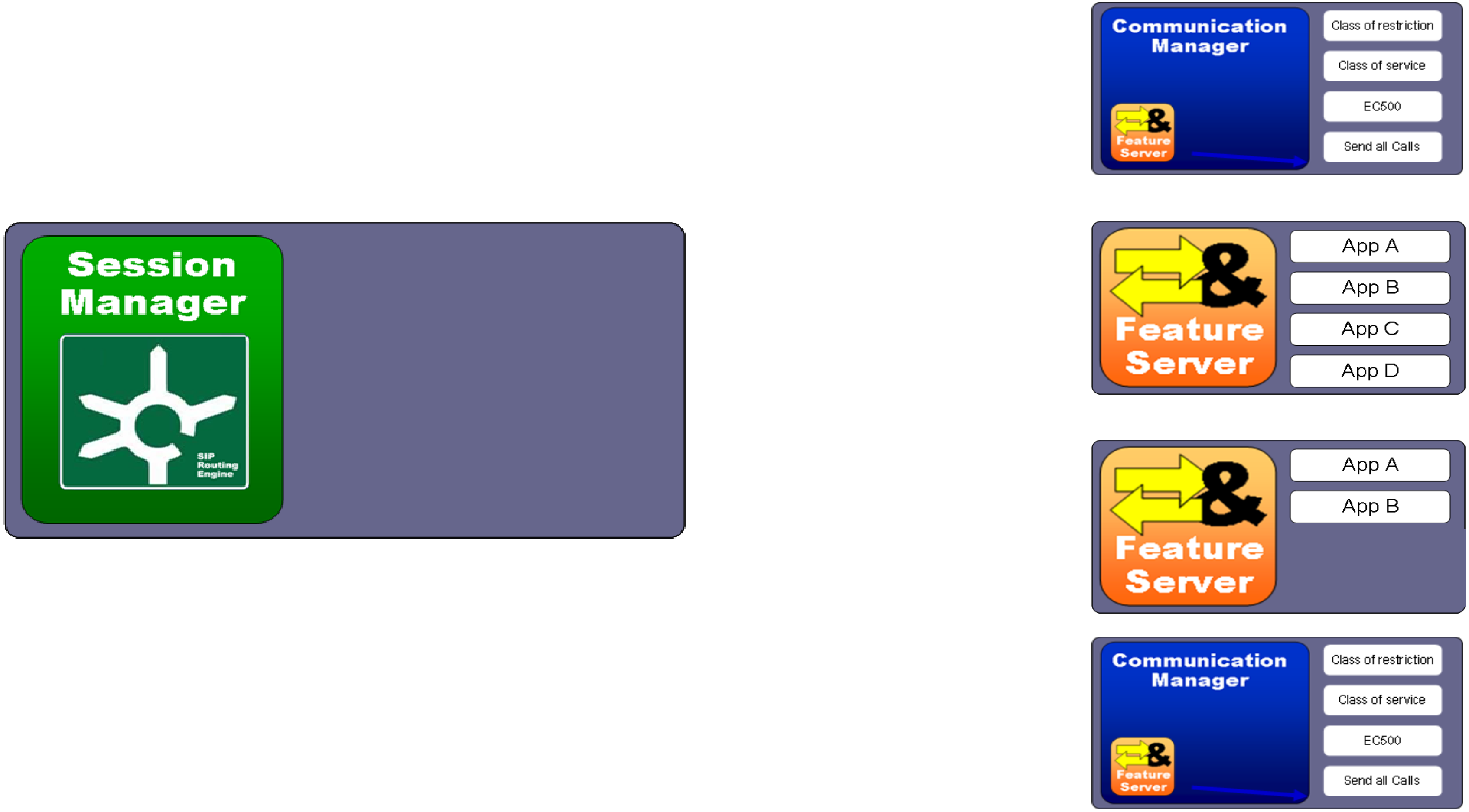
- The application handle is required on 3rd party feature servers.

Route: IP:AppD@featureserver



Session Manager and Applications

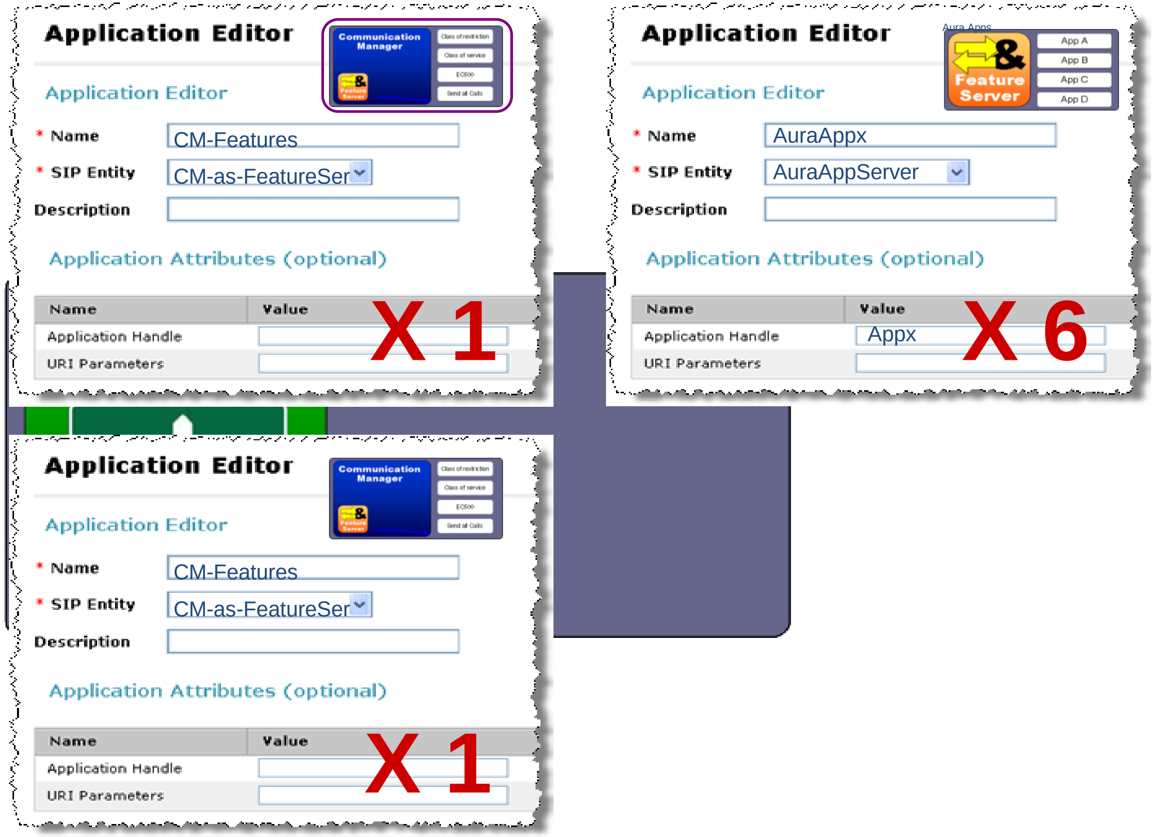
- How many applications will need to be configured on Session Manager?



Session Manager and Applications (continued)

One for each CM. *CM is <u>the</u> app*

Six for other Feature Servers – *4 for 1, 2 for the other*



Application Editor

Application Editor

* Name: CM-Features

* SIP Entity: CM-as-FeatureSer

Description:

Application Attributes (optional)

Name	Value
Application Handle	
URI Parameters	

X 1

Application Editor

Application Editor

* Name: AuraAppx

* SIP Entity: AuraAppServer

Description:

Application Attributes (optional)

Name	Value
Application Handle	Appx
URI Parameters	

X 6

Application Editor

Application Editor

* Name: CM-Features

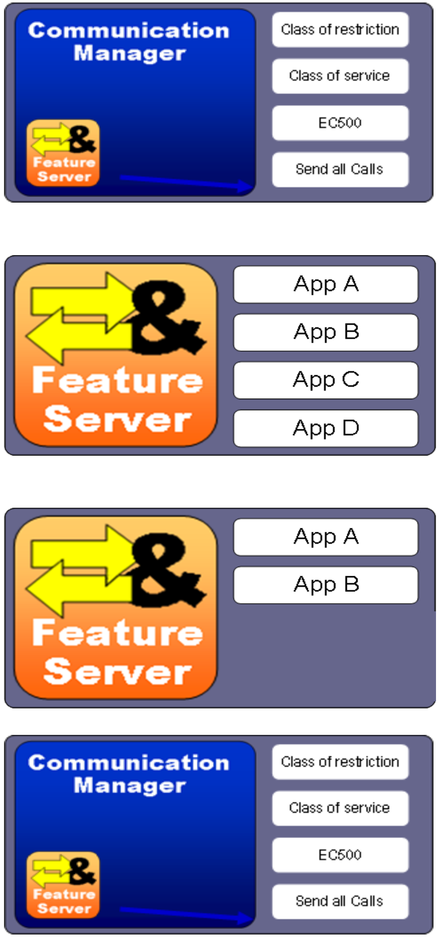
* SIP Entity: CM-as-FeatureSer

Description:

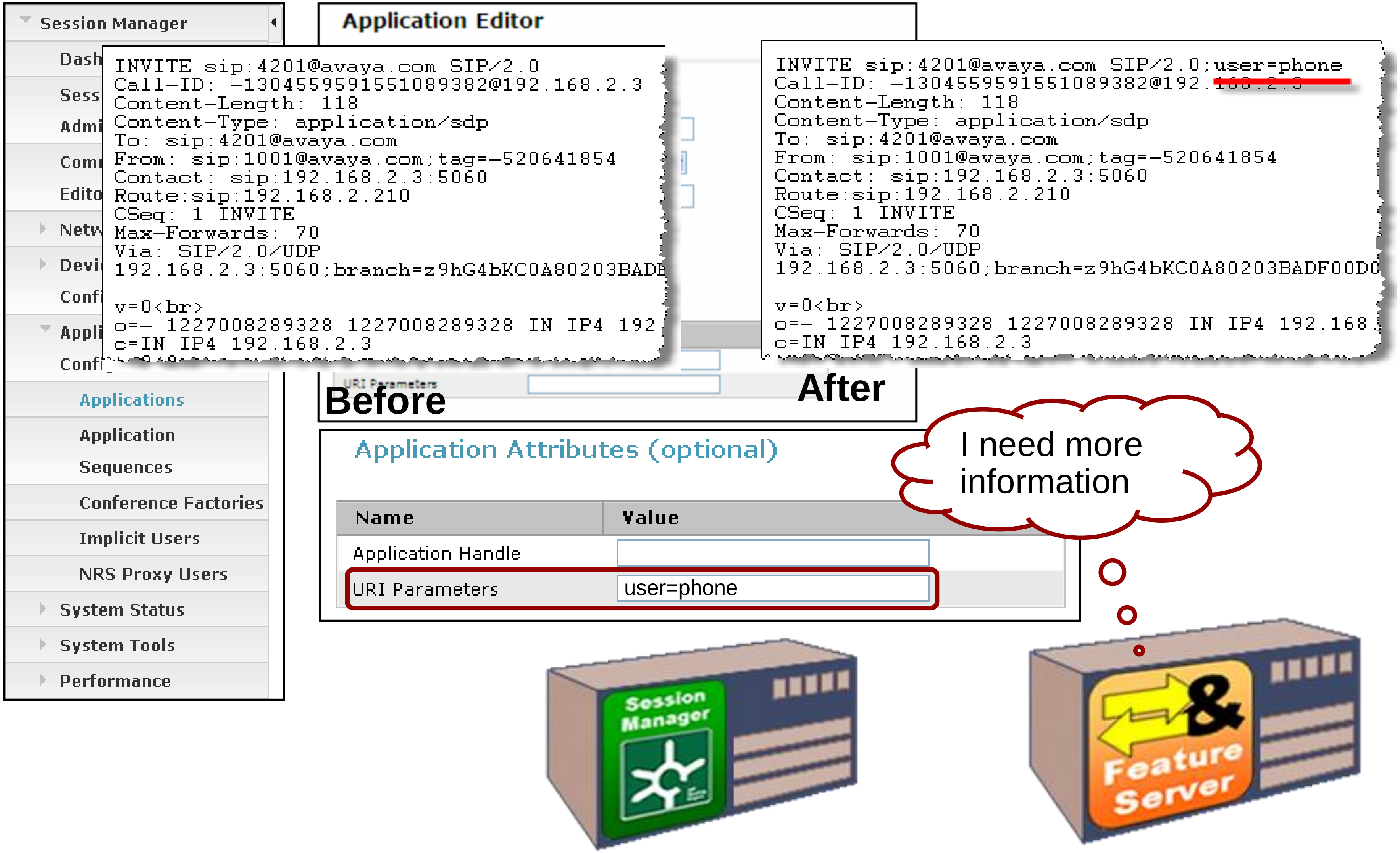
Application Attributes (optional)

Name	Value
Application Handle	
URI Parameters	

X 1



Additional Application Parameters



Before

```
INVITE sip:4201@avaya.com SIP/2.0
Call-ID: -1304559591551089382@192.168.2.3
Content-Length: 118
Content-Type: application/sdp
To: sip:4201@avaya.com
From: sip:1001@avaya.com;tag=-520641854
Contact: sip:192.168.2.3:5060
Route:sip:192.168.2.210
CSeq: 1 INVITE
Max-Forwards: 70
Via: SIP/2.0/UDP
192.168.2.3:5060;branch=z9hG4bKC0A80203BADE

v=0<br>
o=- 1227008289328 1227008289328 IN IP4 192
c=IN IP4 192.168.2.3
```

After

```
INVITE sip:4201@avaya.com SIP/2.0;user=phone
Call-ID: -1304559591551089382@192.168.2.3
Content-Length: 118
Content-Type: application/sdp
To: sip:4201@avaya.com
From: sip:1001@avaya.com;tag=-520641854
Contact: sip:192.168.2.3:5060
Route:sip:192.168.2.210
CSeq: 1 INVITE
Max-Forwards: 70
Via: SIP/2.0/UDP
192.168.2.3:5060;branch=z9hG4bKC0A80203BADF00D0

v=0<br>
o=- 1227008289328 1227008289328 IN IP4 192.168
c=IN IP4 192.168.2.3
```

Application Attributes (optional)

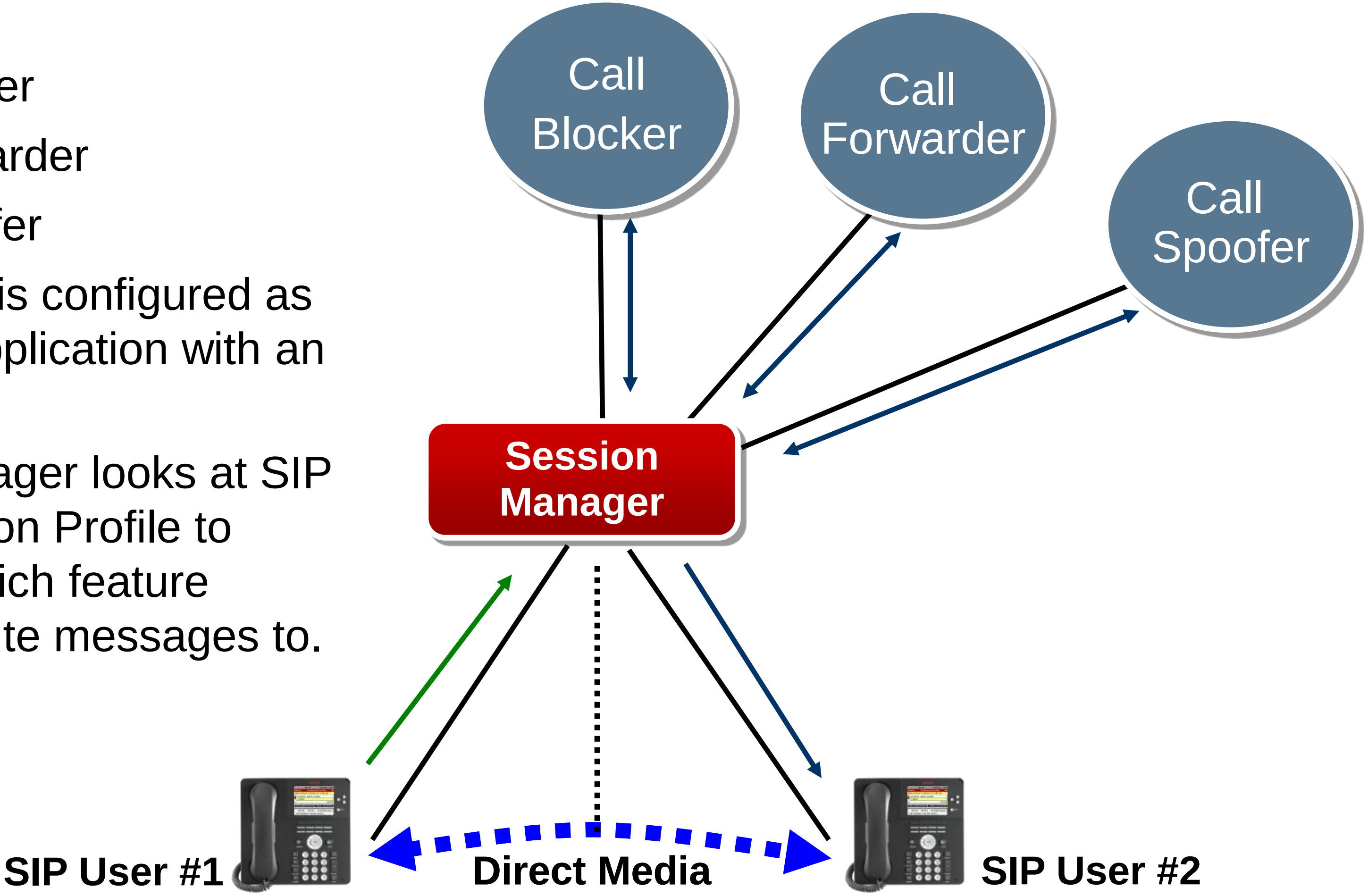
Name	Value
Application Handle	
URI Parameters	user=phone

AVAYA | LEARNING

3rd Party Sequenced Application

Sample Sequenced Java Application

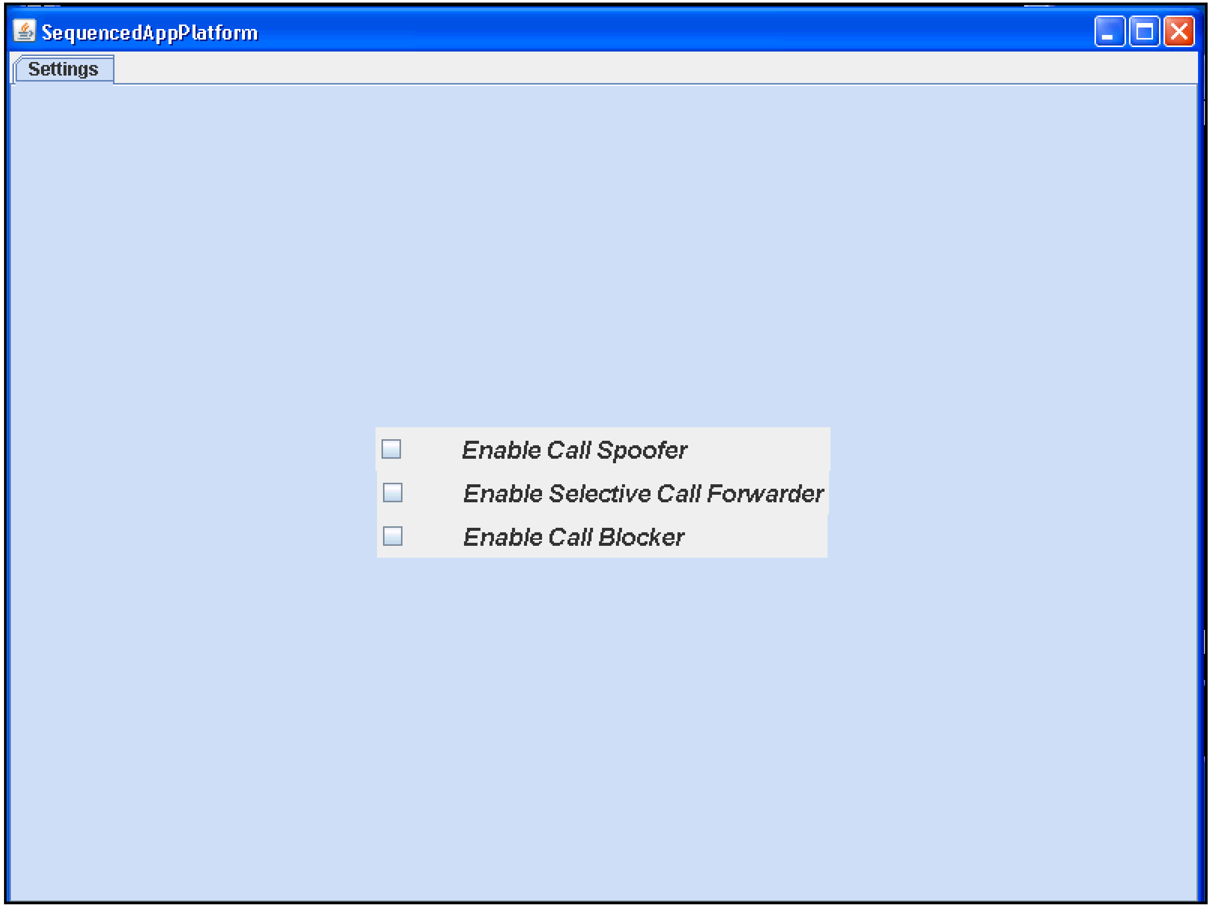
- Provides (3) telephony features:
  - Call Blocker
  - Call Forwarder
  - Call Spoofer
- Each feature is configured as a separate application with an app handle.
- Session Manager looks at SIP Communication Profile to determine which feature servers to route messages to.



Half Call Model

Running SAMPLE Sequenced Application

- 3rd party Java app that: 1. spoofs calls, 2. forwards calls and 3. blocks calls.



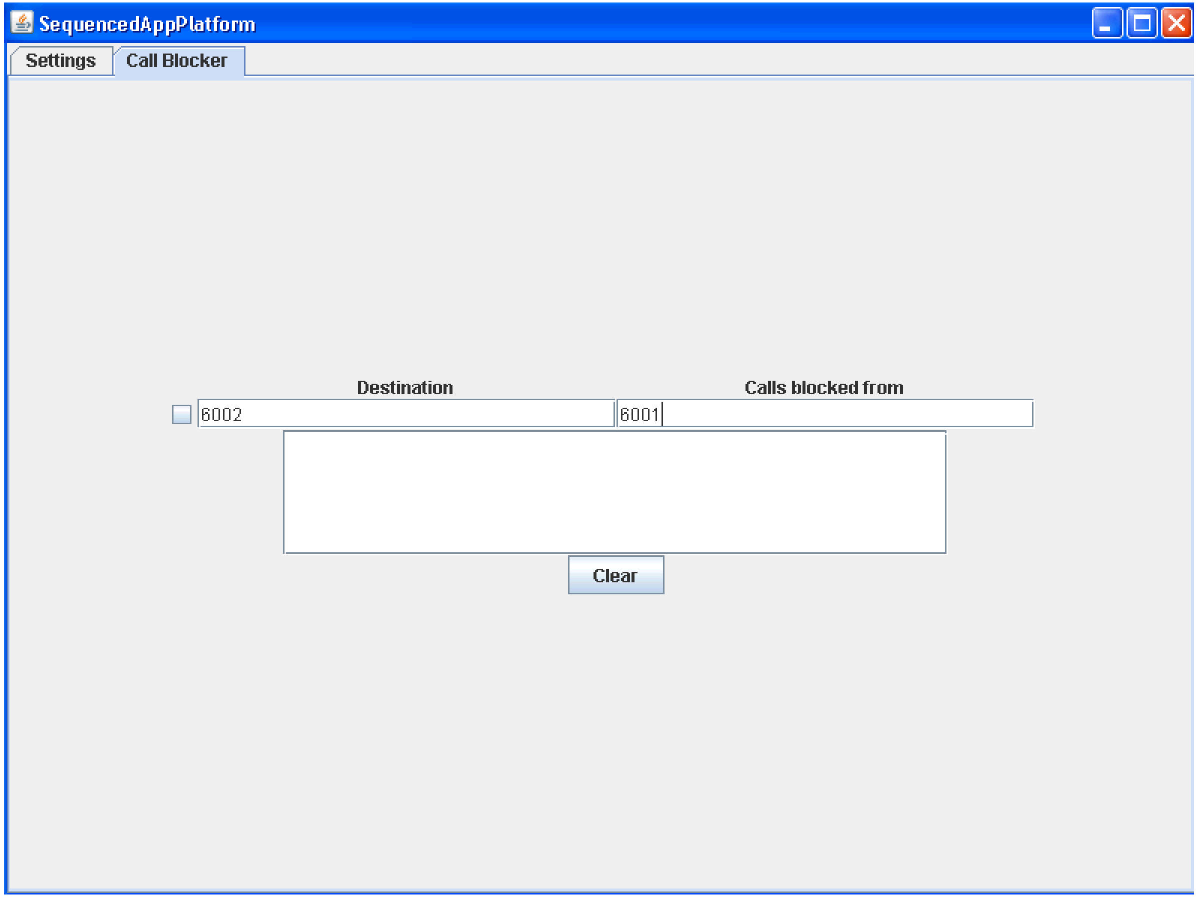
□ Enable Call Spoofer

□ Enable Selective Call Forwarder

□ Enable Call Blocker

Application Sequencing: Origination Vs. Termination ?

CSECallBlocker – This is a terminating app administered on the phone the call is made to. This application can block calls from a given number to the number this application is administered.

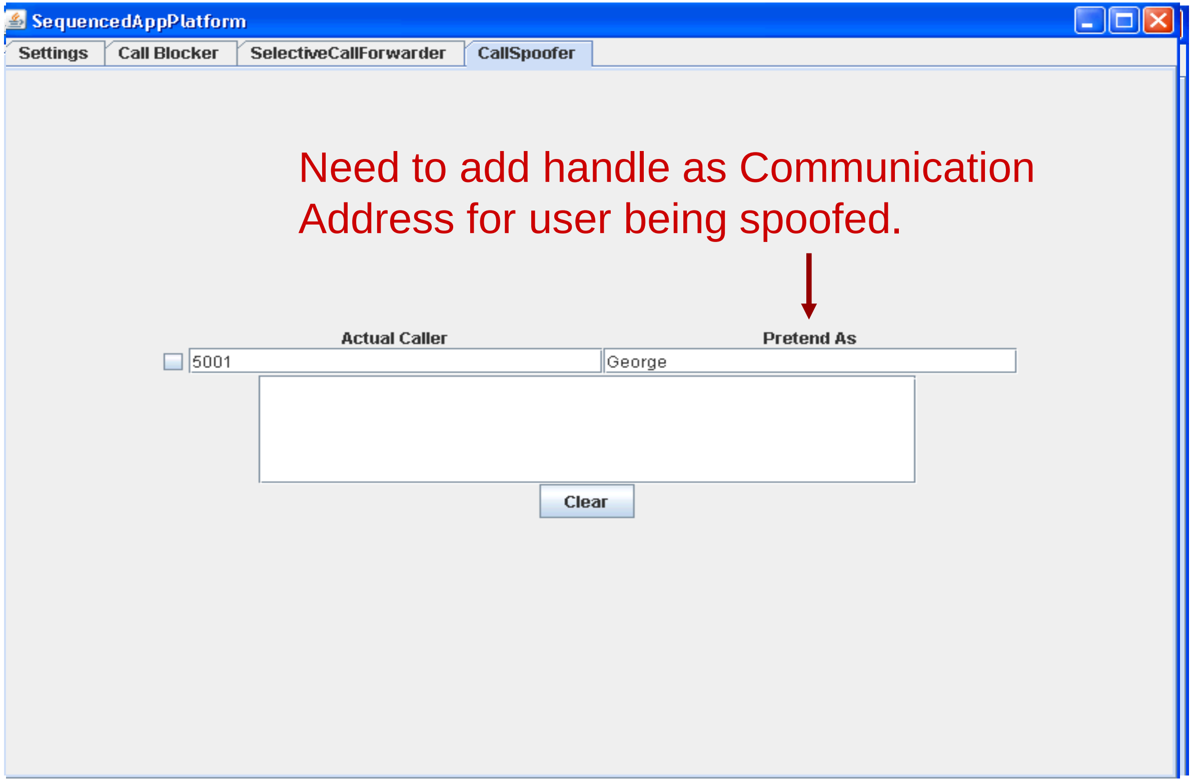


	Destination	Calls blocked from
□	6002	6001

Must add Application Handle - CSECallBlocker

Application Sequencing: Origination Vs. Termination ? (continued)

CSECallSpoofer – Origination. This application changes the identity of the phone placing an outbound call.



Need to add handle as Communication Address for user being spoofed.

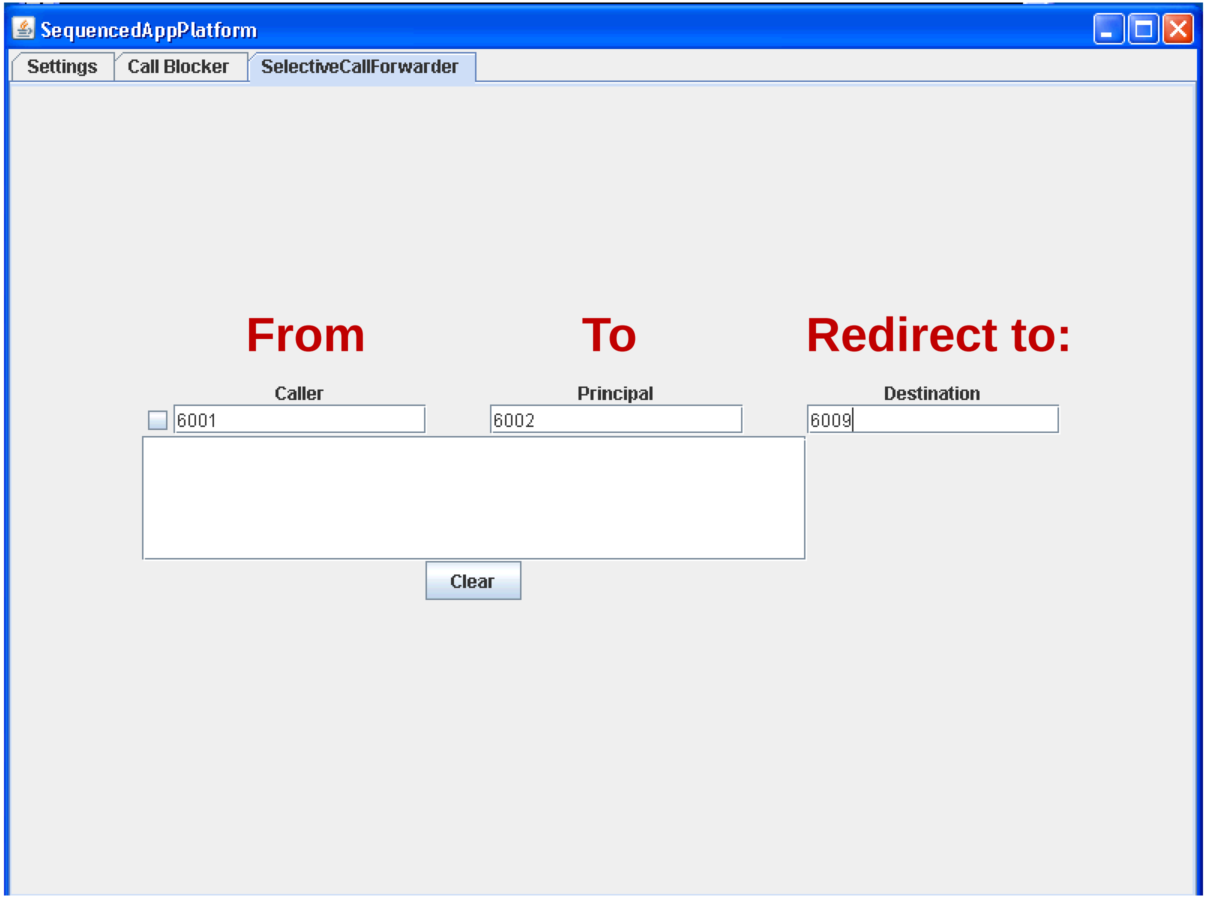
Actual Caller	Pretend As
5001	George

Must add Application Handle - CSECallSpoofer

Application Sequencing: Origination Vs. Termination ? (continued)

CSEsCallForwarder – This is a terminating app, administered on the phone that the call is made to. This application can forward calls from a given number to another number.

SampleSequencedApps.jar



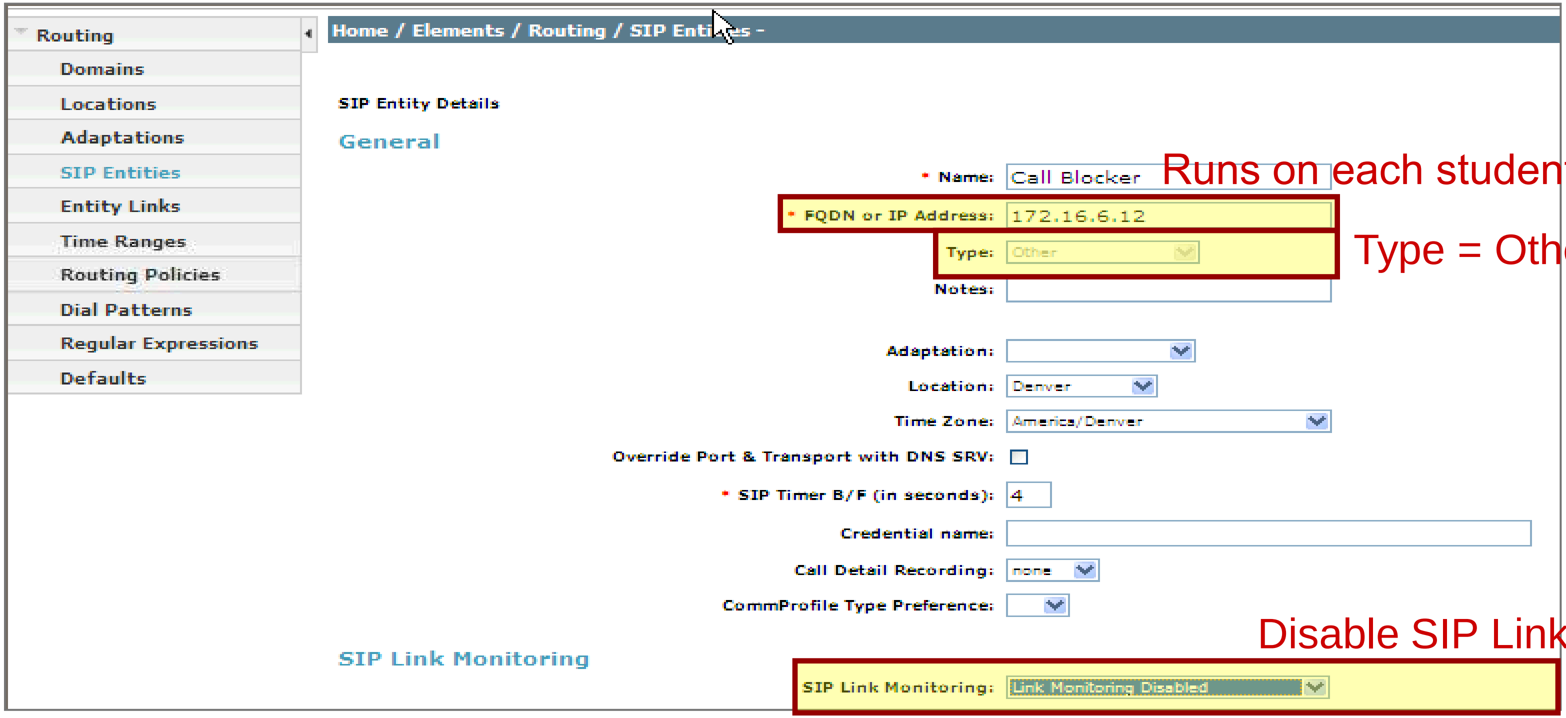
From To Redirect to:

	Caller	Principal	Destination
□	6001	6002	6009

Must add Application Handle - CSEsCallForwarder

Configuring the New Feature Server

- Create a SIP Entity for the new Feature Server



SIP Entity Details

General

* Name: Call Blocker

* FQDN or IP Address: 172.16.6.12

Type: Other

Notes:

Adaptation:

Location: Denver

Time Zone: America/Denver

Override Port & Transport with DNS SRV: □

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

SIP Link Monitoring

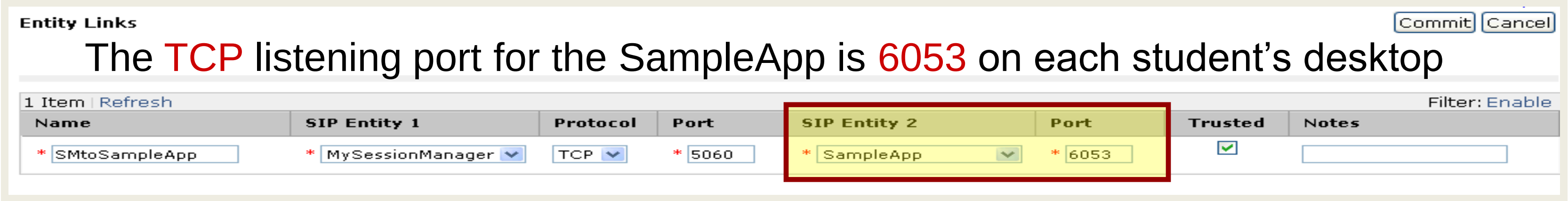
SIP Link Monitoring: Link Monitoring Disabled

Runs on each student’s Desktop

Type = Other

Disable SIP Link Monitoring

Create an Entity Link between ‘MySessionManager’ and the new Feature Server



Entity Links

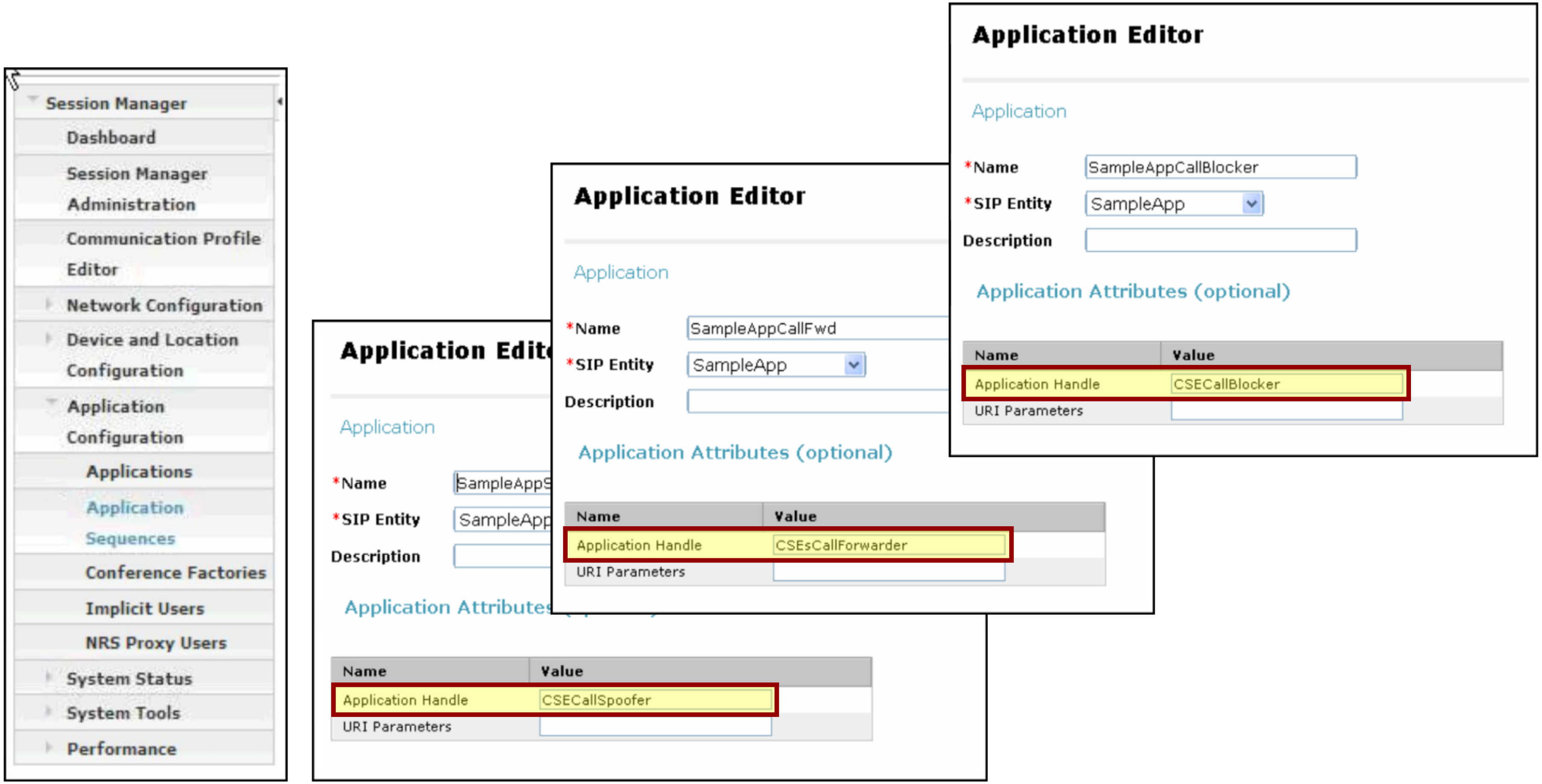
The TCP listening port for the SampleApp is 6053 on each student’s desktop

1 Item | Refresh   Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* SMtoSampleApp	* MySessionManager	TCP	* 5060	* SampleApp	* 6053	☑	

Defining the Application

- Each feature will require an application configuration.



Application Edit

Application

*Name	SampleAppS
*SIP Entity	SampleApp
Description	

Application Attributes

Name	Value
Application Handle	CSECallSpoofer
URI Parameters	

Application Editor

Application

*Name	SampleAppCallFwd
*SIP Entity	SampleApp
Description	

Application Attributes (optional)

Name	Value
Application Handle	CSEsCallForwarder
URI Parameters	

Application Editor

Application

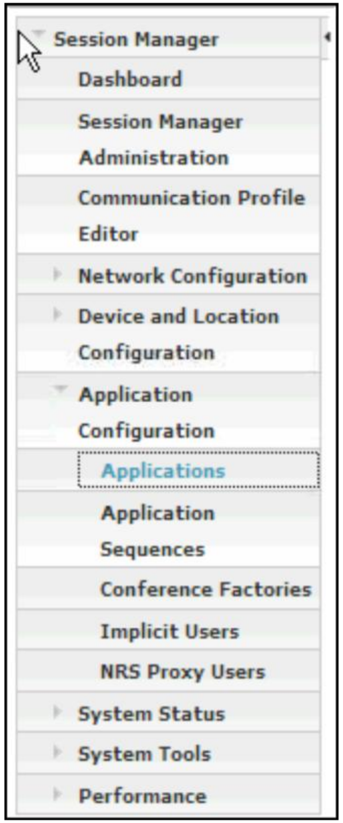
*Name	SampleAppCallBlocker
*SIP Entity	SampleApp
Description	

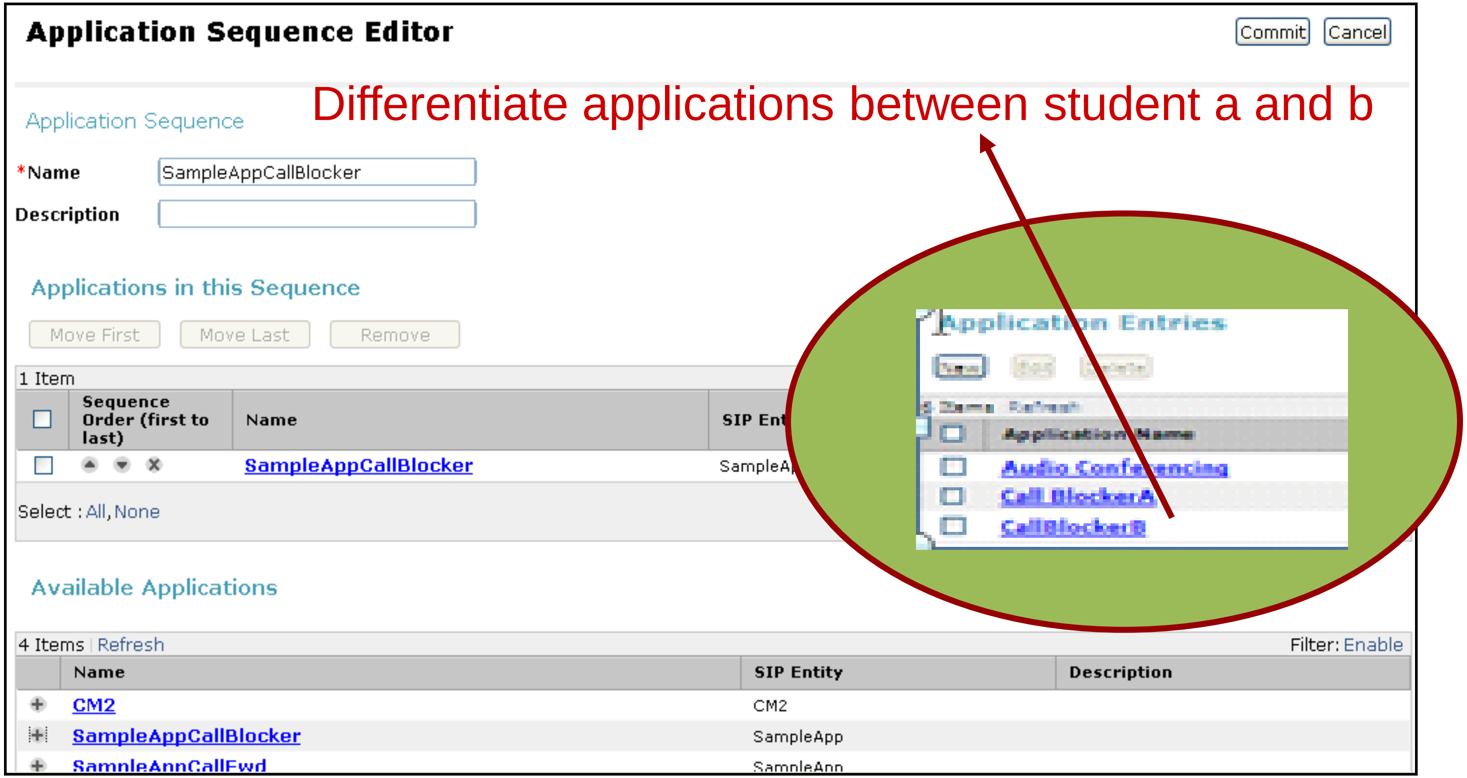
Application Attributes (optional)

Name	Value
Application Handle	CSECallBlocker
URI Parameters	

Create an Application Sequence for Call Blocker

- Select Session Manager from Elements Menu >> Application Sequences





Differentiate applications between student a and b

Application Sequence Editor

Application Sequence

*Name: SampleAppCallBlocker

Description:

Applications in this Sequence

1 Item

☐	Sequence Order (first to last)	Name	SIP Ent
☐	▲ ▼ ✕	SampleAppCallBlocker	SampleA

Select : All, None

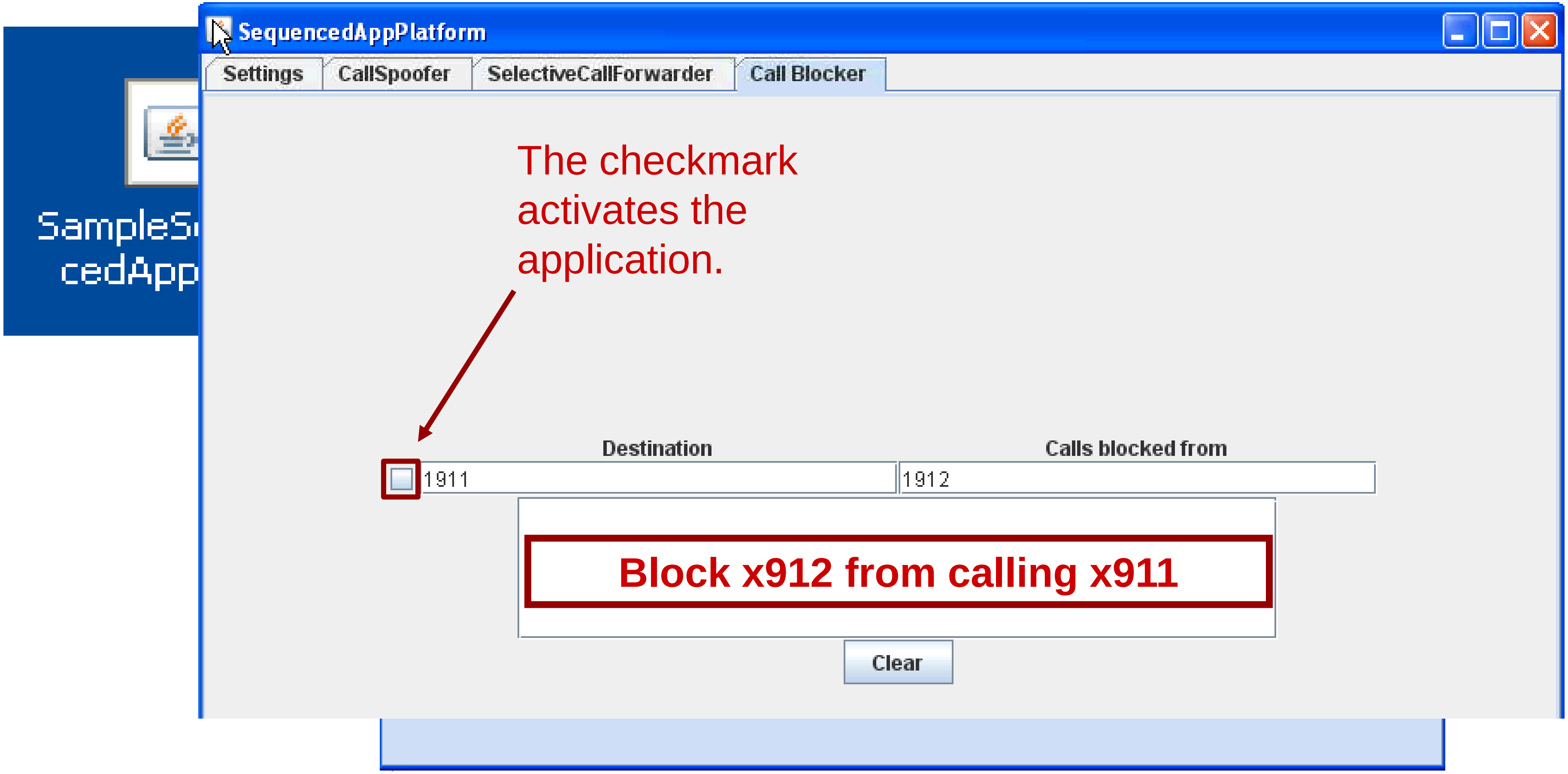
☐	Application Name
☐	Audio Conferencing
☐	Call BlockerA
☐	CallBlockerB

Available Applications

4 Items | Refresh — Filter: Enable

	Name	SIP Entity	Description
+	CM2	CM2	
+	SampleAppCallBlocker	SampleApp	
+	SampleAppCallFwd	SampleApp	

Run the Application – Call Blocker

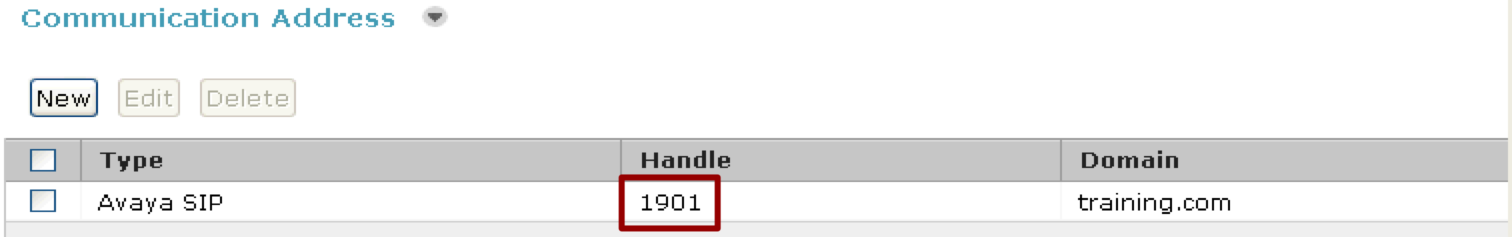


The checkmark activates the application.

	Destination	Calls blocked from
□	1911	1912

Block x912 from calling x911

Assign the New Application Sequence



Communication Address

□	Type	Handle	Domain
□	Avaya SIP	1901	training.com

Select : All, None

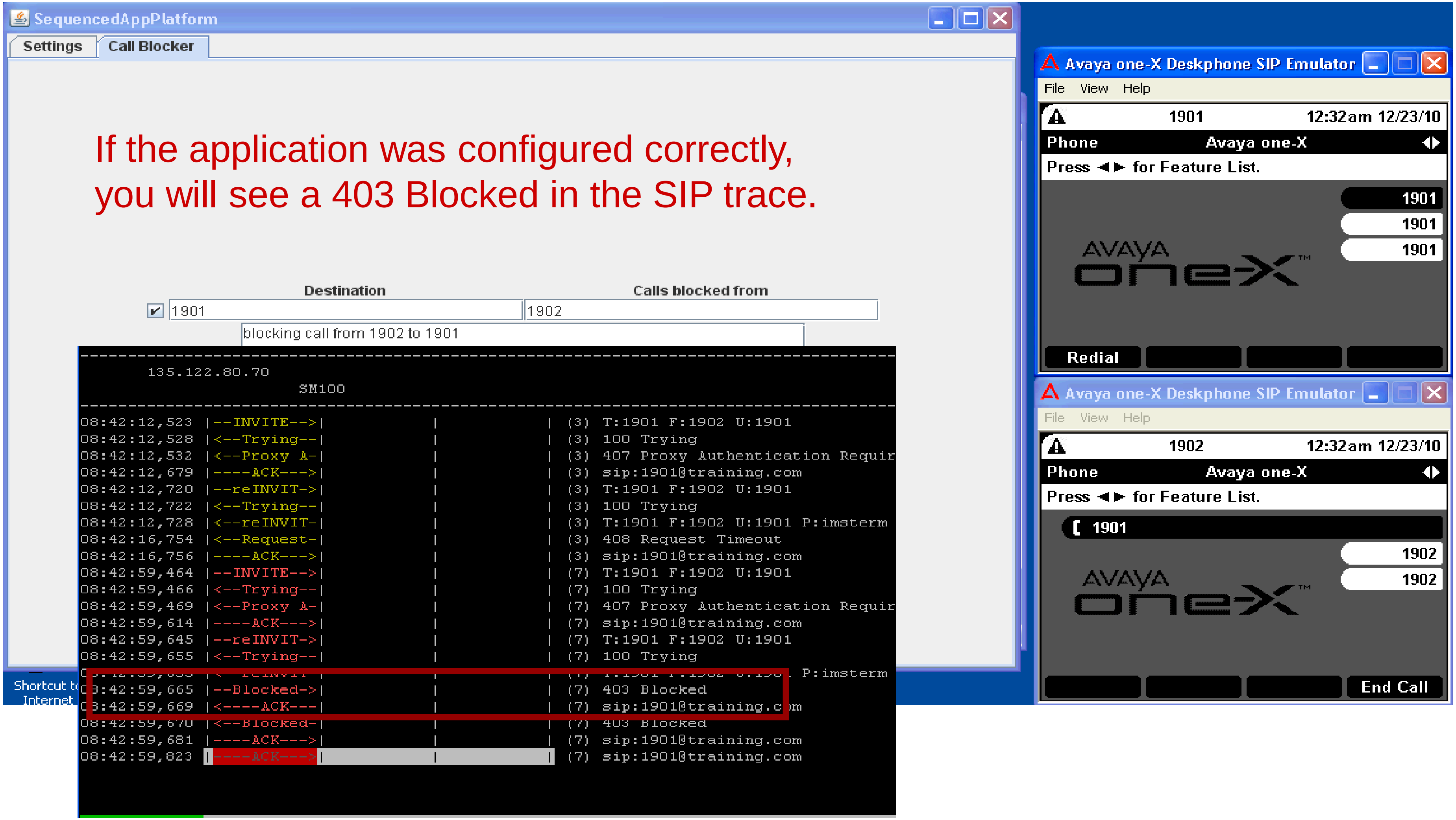
Is Call Blocker an Origination or Termination Application?

Exercise: Implement Sample Application CSECallBlocker

- Block x912 from calling x911 using the Sample App feature called CSECallBlocker.

Step	Action
1	Go to desktop and find the SampleSequencedApp.jar Activate each feature by clicking on the box
2	From the Routing Menu select SIP Entities: Define the SIP Entity (**use desktop IP**) Student a: 172.16.x.11 Student b: 172.16.x.12
3	Define the Entity Link (port 6053/TCP)
4	Define the Application Name: Call Blocker A/B SIP Entity: Select the SIP Entity you've created Add **CSECallBlocker** in the application handle Commit
5	Define the Application Sequence Add the Call Blocker Application by clicking on the **+**
6	Assign the Application Sequence to the User x911/x921 as Termination

Viewing Results



If the application was configured correctly, you will see a 403 Blocked in the SIP trace.

	Destination	Calls blocked from
☑	1901	1902

blocking call from 1902 to 1901

```
--------------------------------------------------------------------------------
       135.122.80.70
                       SM100
--------------------------------------------------------------------------------
08:42:12,523 |--INVITE-->|           |           | (3) T:1901 F:1902 U:1901
08:42:12,528 |<--Trying--|           |           | (3) 100 Trying
08:42:12,532 |<--Proxy A-|           |           | (3) 407 Proxy Authentication Requir
08:42:12,679 |----ACK--->|           |           | (3) sip:1901@training.com
08:42:12,720 |--reINVIT->|           |           | (3) T:1901 F:1902 U:1901
08:42:12,722 |<--Trying--|           |           | (3) 100 Trying
08:42:12,728 |<--reINVIT-|           |           | (3) T:1901 F:1902 U:1901 P:imsterm
08:42:16,754 |<--Request-|           |           | (3) 408 Request Timeout
08:42:16,756 |----ACK--->|           |           | (3) sip:1901@training.com
08:42:59,464 |--INVITE-->|           |           | (7) T:1901 F:1902 U:1901
08:42:59,466 |<--Trying--|           |           | (7) 100 Trying
08:42:59,469 |<--Proxy A-|           |           | (7) 407 Proxy Authentication Requir
08:42:59,614 |----ACK--->|           |           | (7) sip:1901@training.com
08:42:59,645 |--reINVIT->|           |           | (7) T:1901 F:1902 U:1901
08:42:59,655 |<--Trying--|           |           | (7) 100 Trying
08:42:59,6[illegible] |<--reINVIT-|           |           | (7) T:1901 F:1902 U:1901 P:imsterm
08:42:59,665 |--Blocked->|           |           | (7) 403 Blocked
08:42:59,669 |<----ACK---|           |           | (7) sip:1901@training.com
08:42:59,670 |<--Blocked-|           |           | (7) 403 Blocked
08:42:59,681 |----ACK--->|           |           | (7) sip:1901@training.com
08:42:59,823 |----ACK--->|           |           | (7) sip:1901@training.com
```

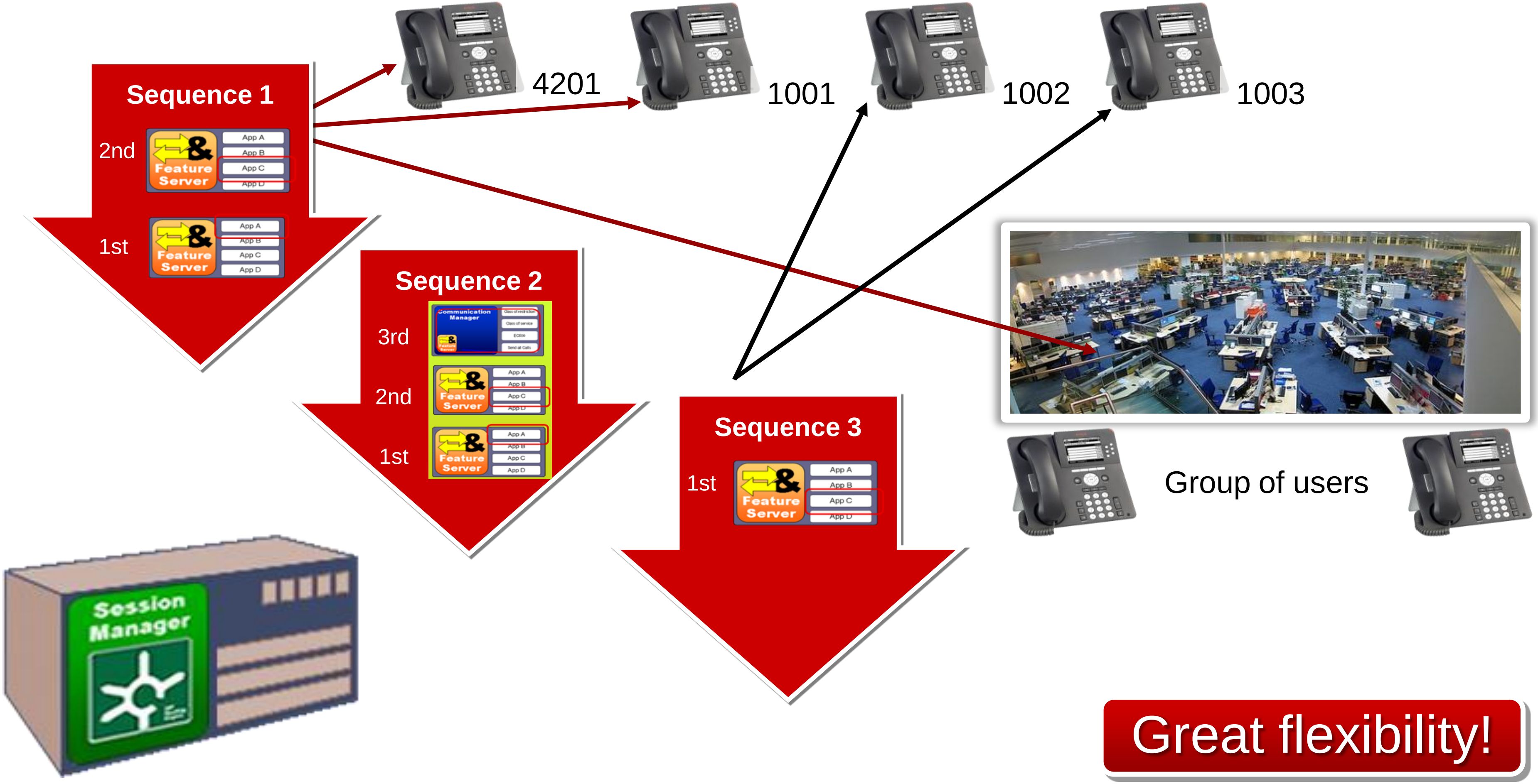
Multiple Applications in a Sequence

Application Sequences

Multiple application sequences give us the flexibility to pick and choose, mix and match features for users!

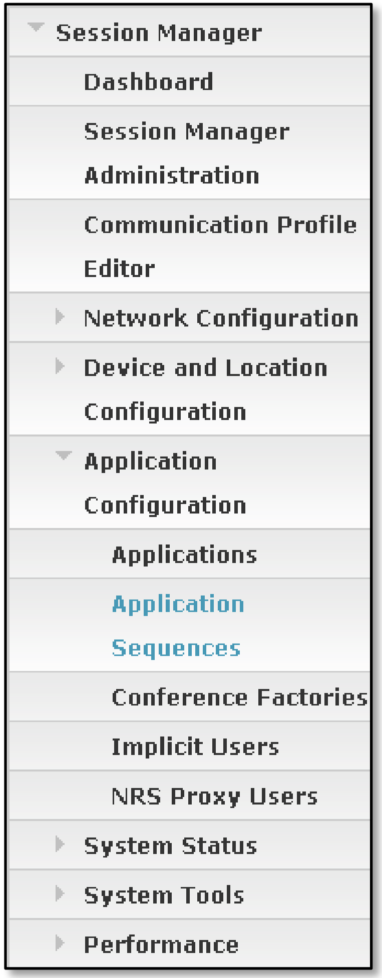
A Sequence is a Template

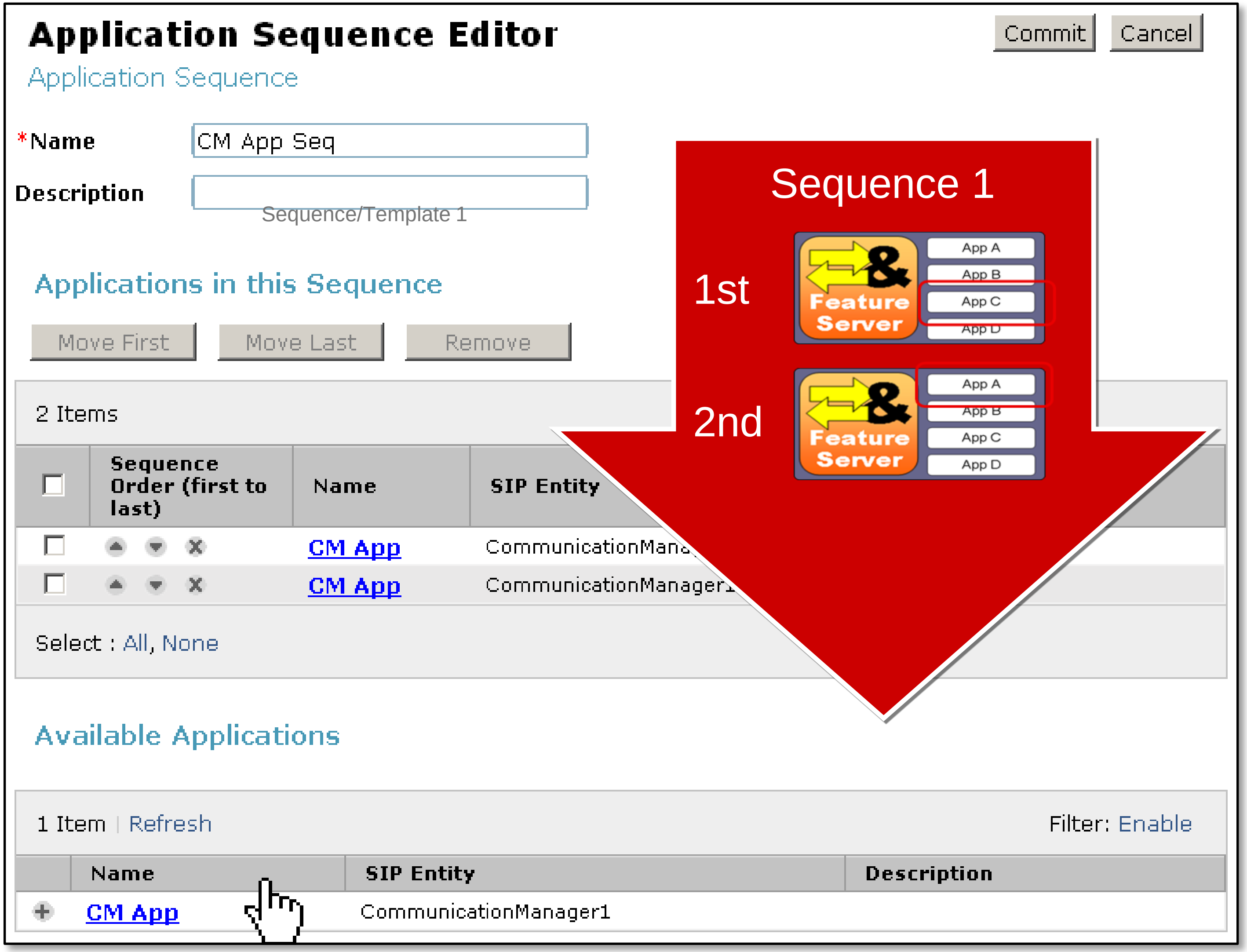
- Once a sequence is created it can be applied multiple times
- Different sequences can be applied to different types of users



Great flexibility!

Administering an Application Sequence





Application Sequence Editor

Application Sequence

*Name: CM App Seq

Description:

Sequence/Template 1

Applications in this Sequence

2 Items

□	Sequence Order (first to last)	Name	SIP Entity
□	▲ ▼ ✕	CM App	CommunicationMana
□	▲ ▼ ✕	CM App	CommunicationManager1

Select : All, None

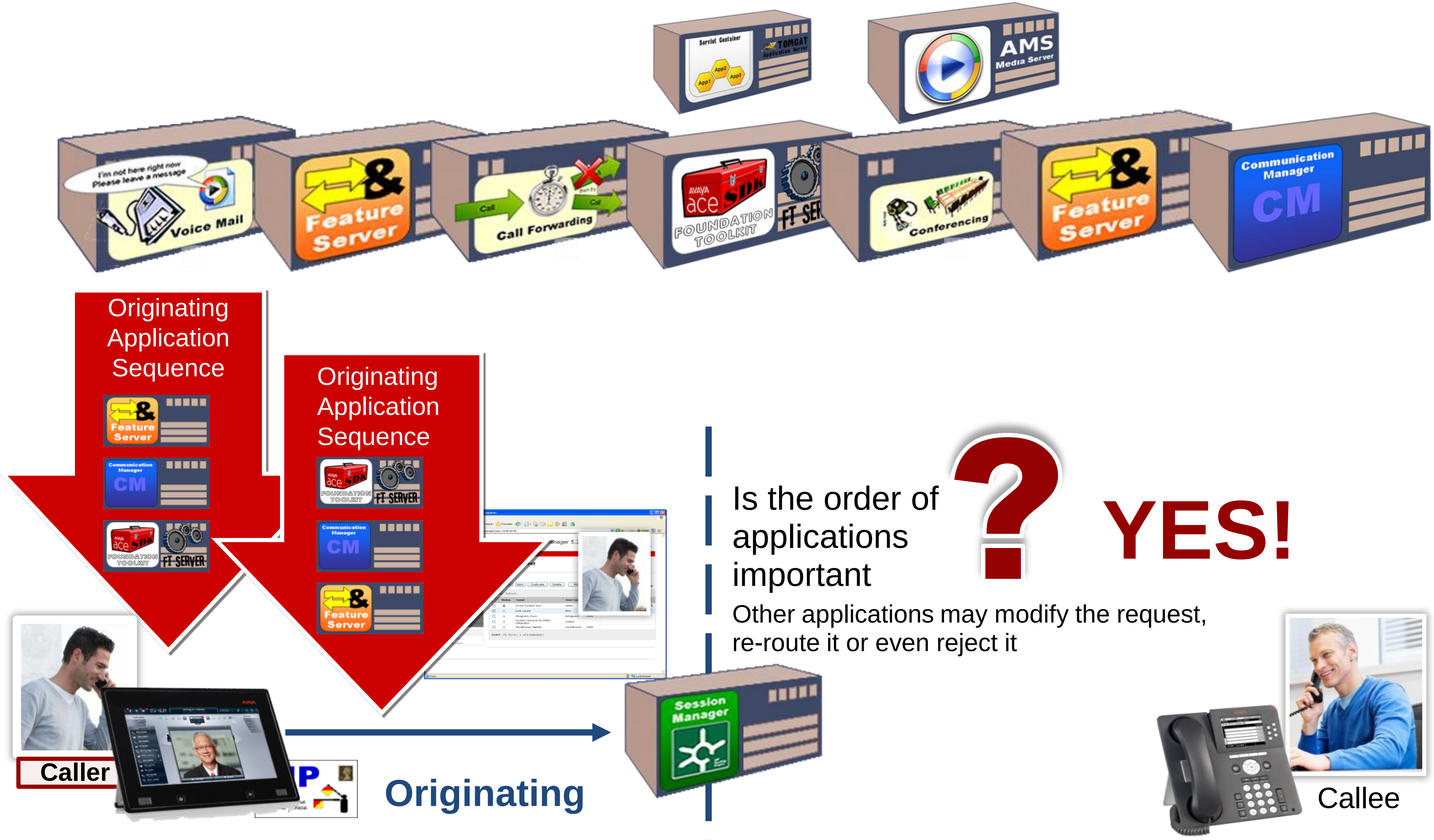
Available Applications

1 Item | Refresh

Filter: Enable

	Name	SIP Entity	Description
+	CM App	CommunicationManager1	

Order of Application Sequence



Originating Application Sequence

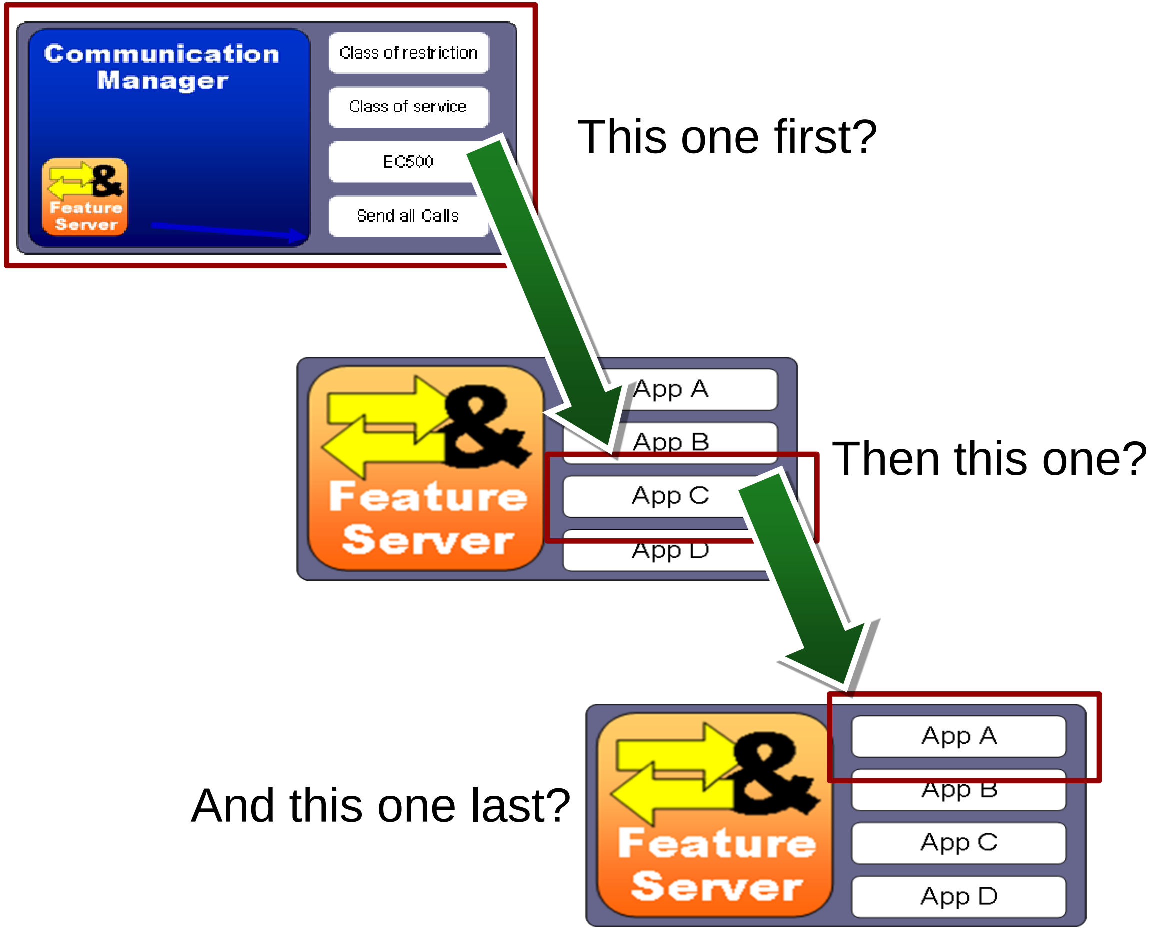
Originating Application Sequence

Originating

Is the order of applications important ? YES!

Other applications may modify the request, re-route it or even reject it

What Combinations Provide Required Outcome?

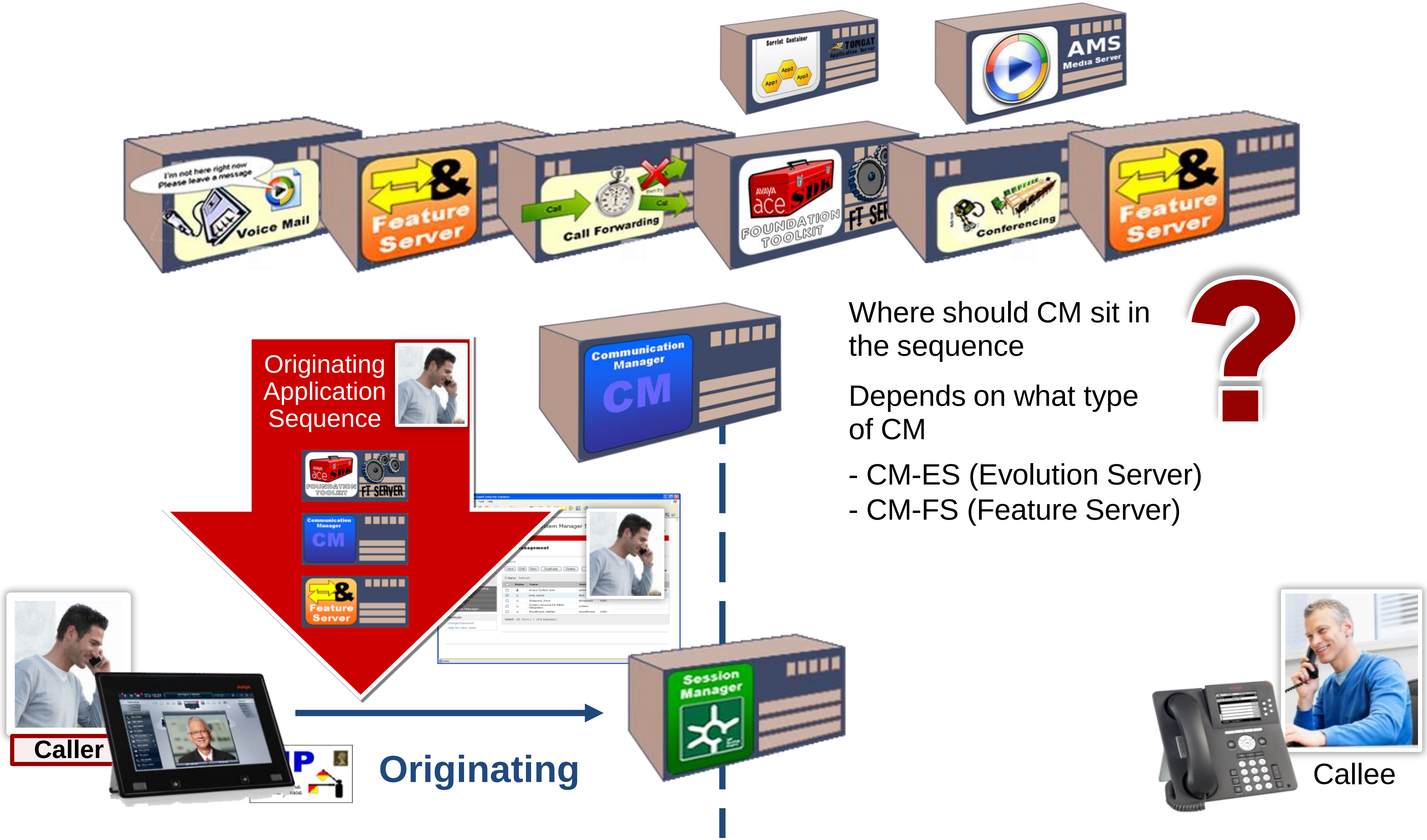


This one first?

Then this one?

And this one last?

Sequence Order



Where should CM sit in the sequence

Depends on what type of CM

- CM-ES (Evolution Server)
- CM-FS (Feature Server)

Rules for Application Sequence Placement for CM

The CM-ES must be last in the origination sequence, and first in the termination sequence.

The CM-FS must be first in the in the origination sequence and the termination sequence.

Lesson Summary

You have completed the following lesson objective:

- Review the nature of sequenced applications, and how they are administered.

AVAYA | LEARNING

Administering Features to Non-SIP Users

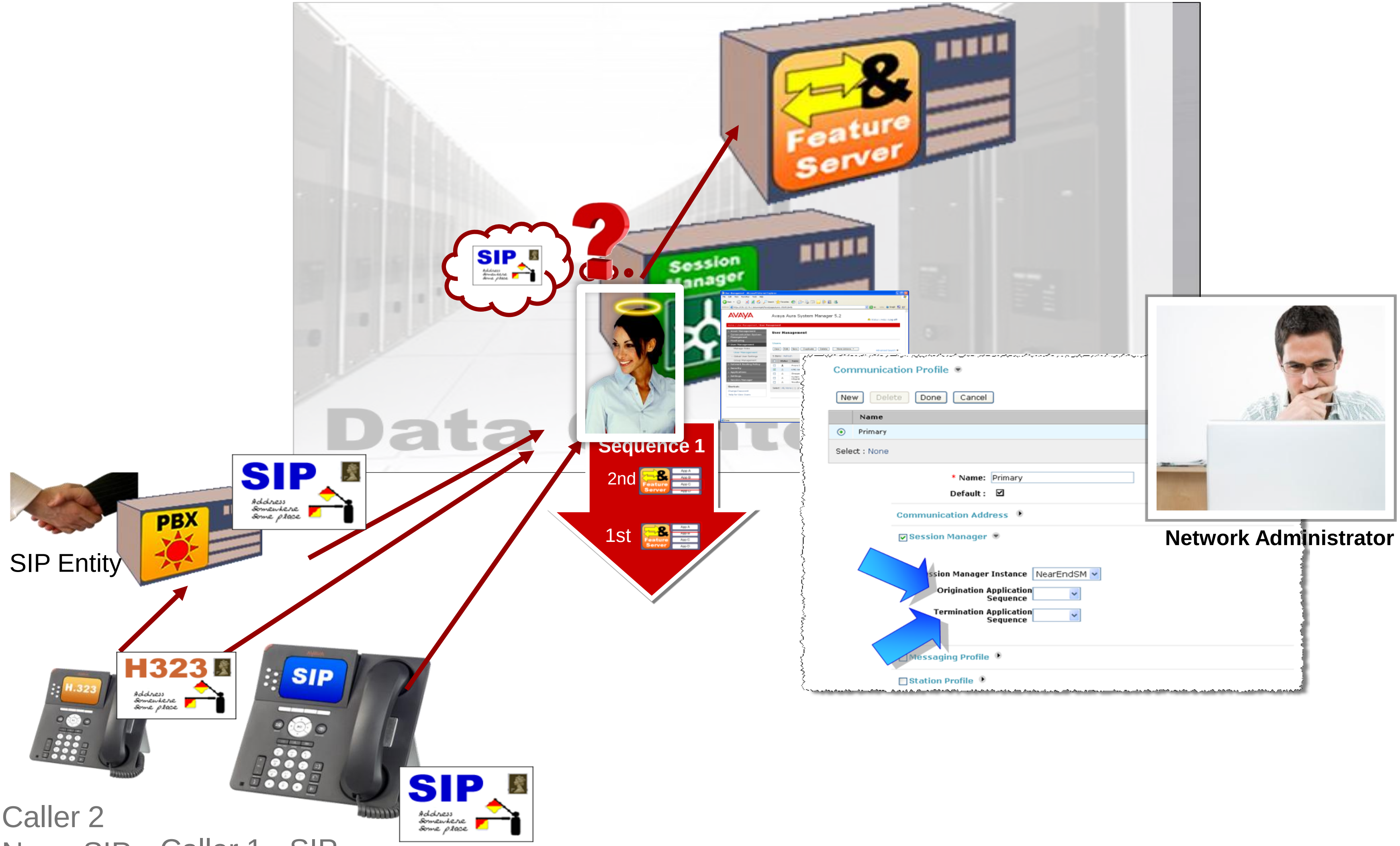
Lesson Objectives

After you complete this course you will be able to:

- Apply features to non-SIP users using Implicit Users.

Implicit Users

Non-SIP Phones and Feature Application



Communication Profile

New | Delete | Done | Cancel

	Name
●	Primary

Select : None

* Name: Primary

Default : ☑

Communication Address

☑ Session Manager

Session Manager Instance: NearEndSM

Origination Application Sequence:

Termination Application Sequence:

☐ Messaging Profile

☐ Station Profile

Non-SIP Phones and Feature Application (continued)

1st problem?

SM expects SIP

1st solution?

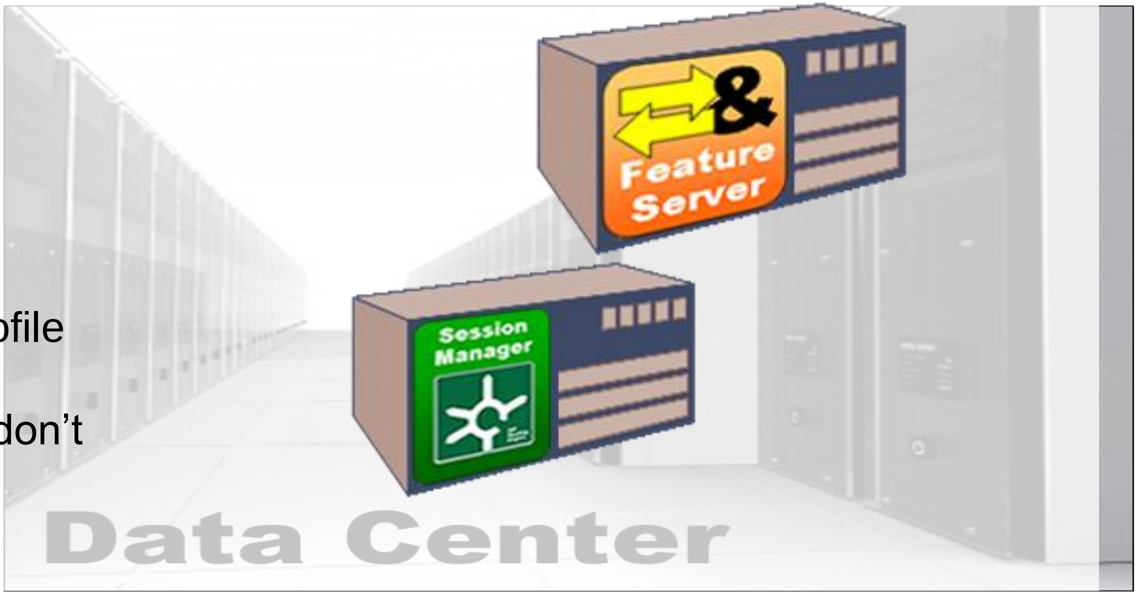
Gateway SIP Entity

2nd problem?

SM checks User Profile
for Sequences.
Non-SIP endpoints don’t
have a User Profile

2st solution?

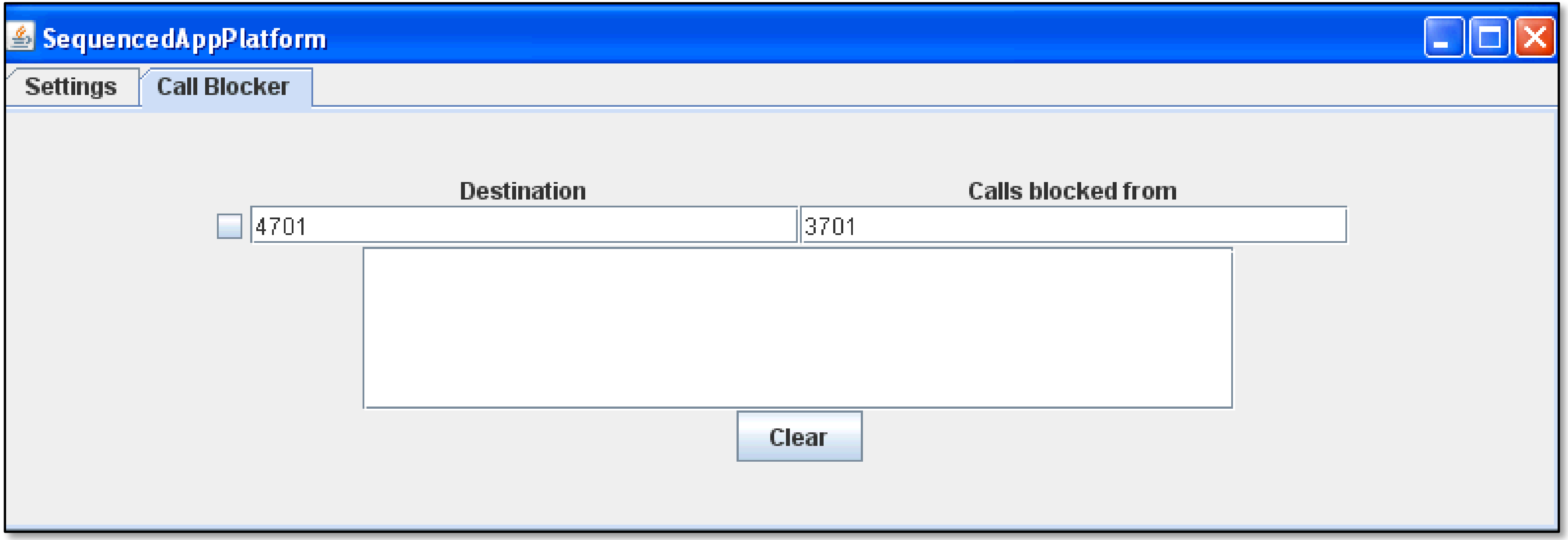
Implicit Users



Caller 2
Non - SIP

Implicit Users-prep

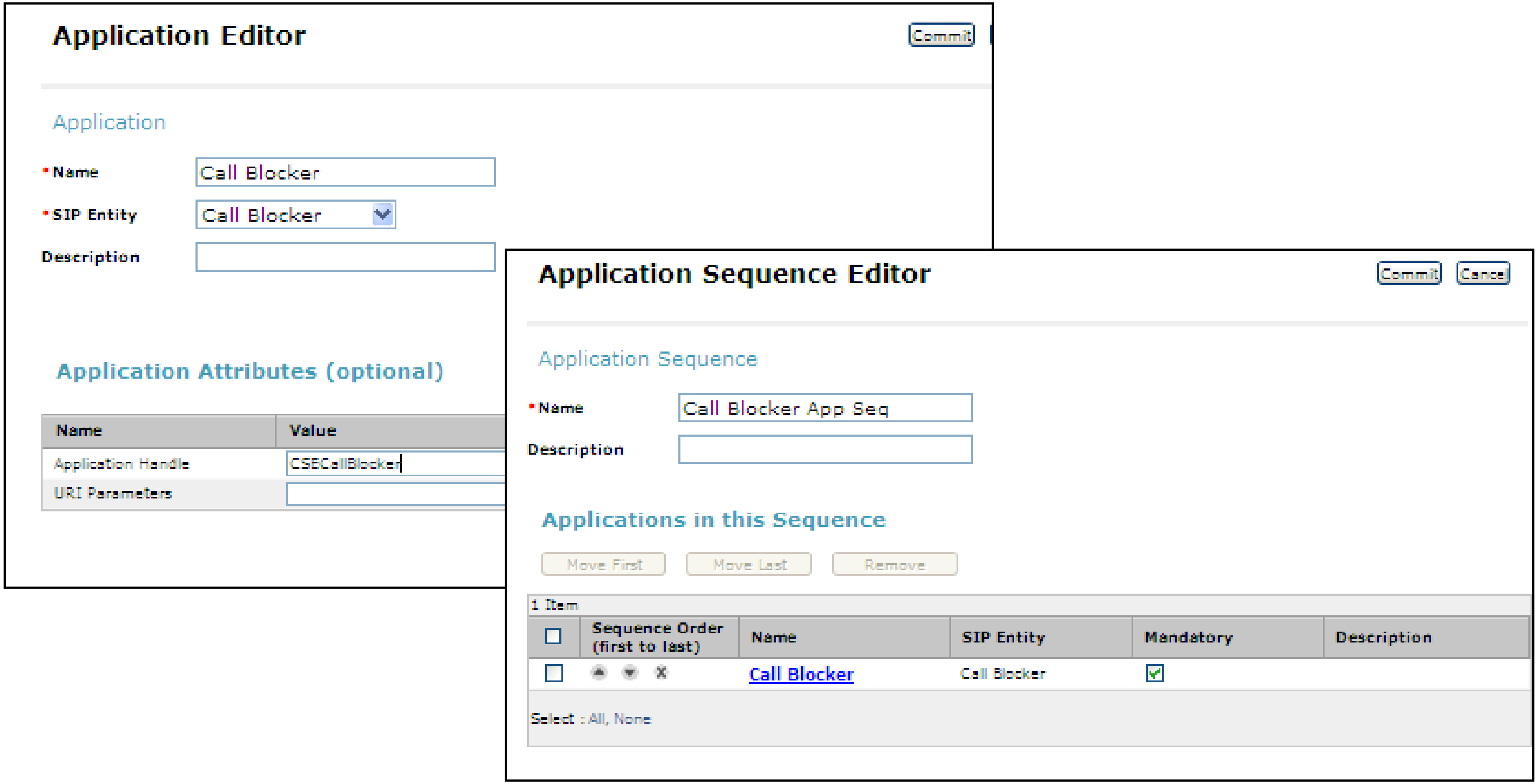
- Configure the Call Blocker app to block your SIP phone from calling your H.323 phone.
- If the application was configured correctly, you will see a 403 Blocked in the SIP trace.



	Destination	Calls blocked from
□	4701	3701

Implicit Users-prep

You will be using the application sequence you’ve created for the Call Blocker App.



Application Editor

Application

*Name: Call Blocker

*SIP Entity: Call Blocker

Description:

Application Attributes (optional)

Name	Value
Application Handle	CSECallBlocker
URI Parameters	

Application Sequence Editor

Application Sequence

*Name: Call Blocker App Seq

Description:

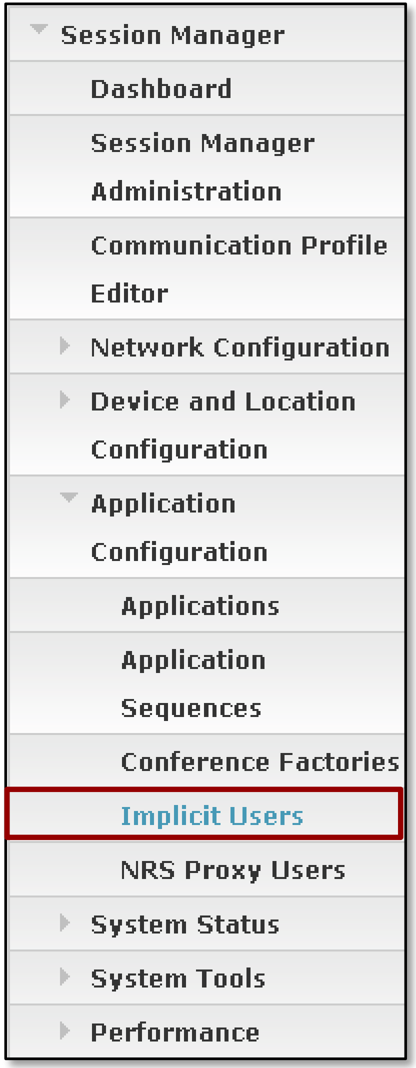
Applications in this Sequence

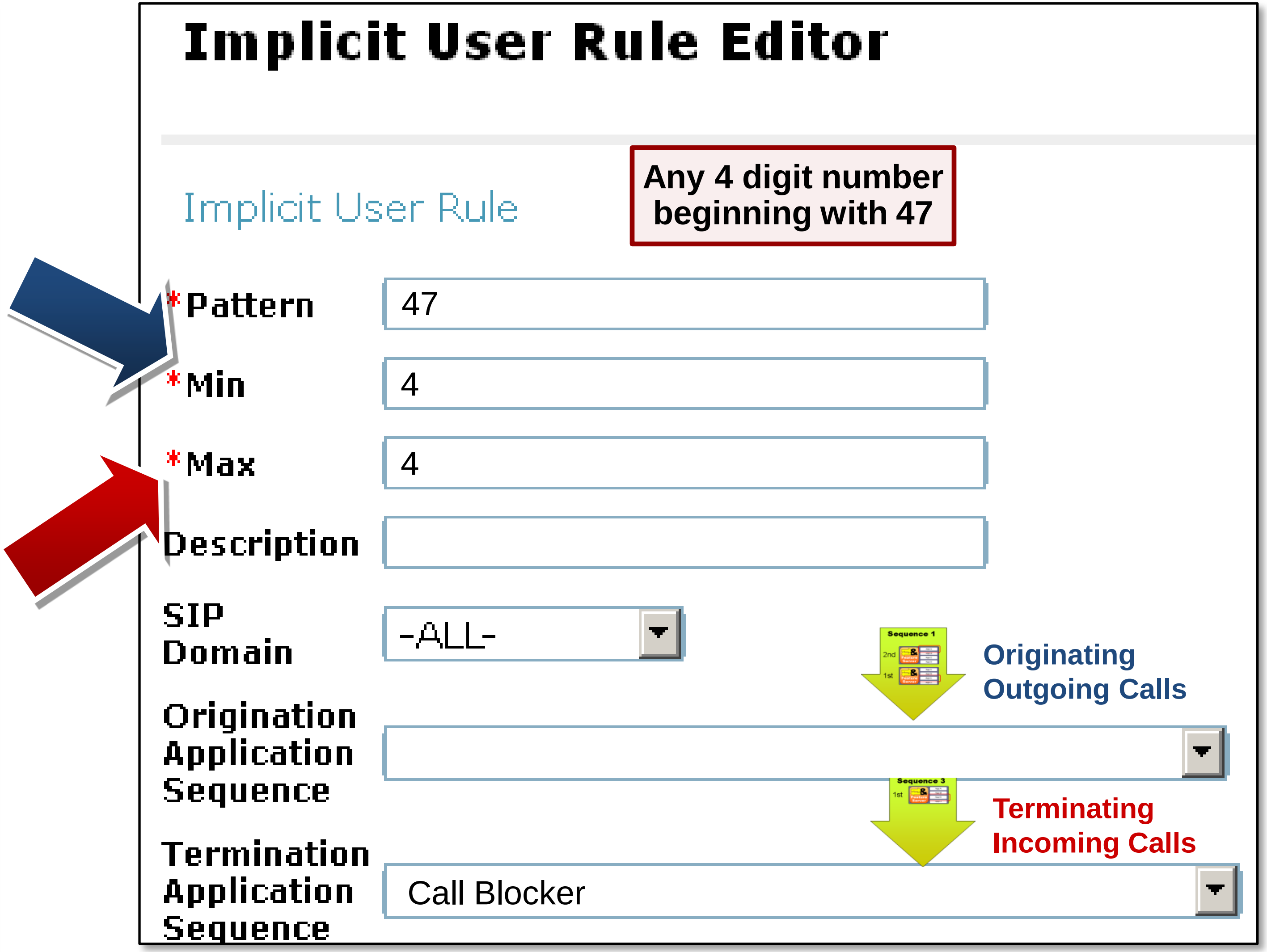
1 Item

□	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
□	▲ ▼ ✗	Call Blocker	Call Blocker	☑	

Select : All, None

Creating an Implicit User for non-SIP Endpoints





Implicit User Rule Editor

Implicit User Rule

Any 4 digit number beginning with 47

*Pattern: 47

*Min: 4

*Max: 4

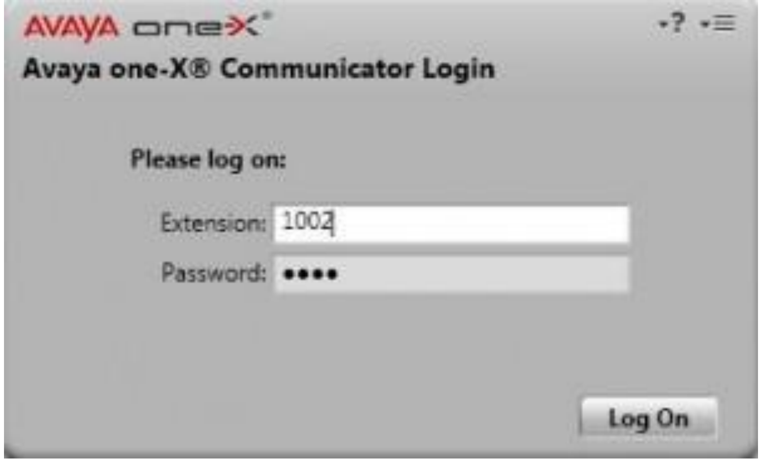
Description:

SIP Domain: -ALL-

Origination Application Sequence:

Termination Application Sequence: Call Blocker

Access the H.323 Phone



Avaya one-X® Communicator Login

Please log on:

Extension: 1002

Password: ••••

Call Server = 172.16.x.53

Password: 123456

Student	Pod 1	Pod 2	Pod 3	Pod 4	Pod 5	Pod 6
Student a	1711	2711	3711	4711	5711	6711
Student b	1721	2721	3721	4721	5721	6721

Exercise: Implicit User

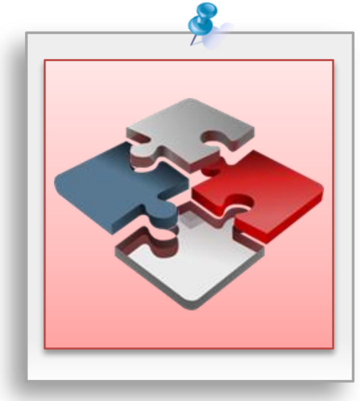
●

Step	Action
1	Make a test call between H.323 and SIP phones to make sure the call completes.
2	Add a rule using Implicit Users to block your SIP x911 or x921 to call your H.323 x711 or x721
3	Modify the settings on the Call Blocker Sample Sequenced Application to block your partner's extension from calling your extension.
4	Apply the application sequence that only contains the Call Blocker app
5	Create an Implicit User Dial Pattern:Your H.323 phone extension (17,27,37,47) Min/Max Length: 4 Assign App sequence to Termination Application Sequence
6	When your Pod partner calls you the call will not go through. Run traceSM to view the call flow.

Lesson Summary

After you complete this course you will be able to:

- Apply features to non-SIP users with Implicit Users.



Module Summary

After completing this module, you will be able to:

- Identify the role of Session Manager in applying features to calls and know how to administer named and sequenced applications.
- Administer Sequenced Applications: Avaya and 3rd Party.
- Administer features to non-SIP users using Implicit Users.

To Learn More

Support and Documentation

- **https://support.avaya.com - Avaya Aura™ Session Manager**
- **Avaya Aura™ Session Manager Overview**
- **Installing and Configuring Avaya Aura Session Manager**
- **Administering Avaya Aura™ Session Manager**
- **Maintaining and Troubleshooting Avaya Aura™ Session Manager**
- **Comparison of Avaya Aura™ SIP Enablement Services and Avaya Aura™ Session Manager 6.x**
- **Administering Avaya Aura™ Communication Manager as a Feature Server**